http://faculty.math.tsinghua.edu.cn/faculty/~ghu/html/catelog0.htm

第一章

习题 1.1

1. 用 2 种颜色的珠子做成有 5 颗珠子项链，问可做出多少种不同的项链？

   解 在学群论前我们没有一般的方法，只能用枚举法。用笔在纸上画一下，用黑白两种珠子，分类进行计算：例如，全白只 1 种，四白一黑 1 种，三白二黑 2 种，…等等，可得总共 8 种。

2. 对正四面体的顶点用 2 种颜色着色，有多少种本质上不同的着色方法？

   解 类似第 1 题，用枚举法可得 5 种。

3. 有 4 个顶点的图共有多少个？互不同构的有多少个？

   解 由本节内容，有 4 个顶点的图共有 64 个图。用分类计数的方法可得共有 11 个互不同构的图。

4. 如何用圆规 5 等分一个圆？

   解 用初等数学的方法求五边形的边长：作一个顶角为 36°、腰长为 1 的等腰三角形，设底边长为 a，则 a 就是十边形的边长，以 a 为半径以单位圆周上任意一点为圆心在圆周上交出两点，则这两点之间的距离就是五边形的边长。

   那么 a 怎么求呢？只要在那个等腰三角形上作一条补助线&#0;底角的角平分线，再利用相似三角形边长成比例的关系，可得 $a=\frac{\sqrt{5}-1}{2}$ ，因而 a 就可作出了。

5. 用根式表示 3 次和 4 次代数方程的根。查看数学手册。因公式较复杂，不在这里列出了。

习题 1.2

1.设 $|A|<\infty$,用二项式定理证明 $\left|2^A\right|=2^{|A|}$.

证 设 $A=\{a_1,a_2,\cdots,a_n\}$,由于 k 元子集的个数为 $\binom{n}{k}$,

所以全部子集的个数(包括空集)为 $\sum_{k=0}^{n}\binom{n}{k}=(1+1)^n=2^n$,

即 $\left|2^A\right|=2^{|A|}$.

2.一个班有93%的人是团员,80%的人担任过社会工作,70%的人受过奖励,问

(1)受过奖励的团员至少占百分之几?

(2)三者兼而有之的人至少占百分之几?

解 设 A 为团员的集合,B 为担任过社会工作的人的集合,C 为受过奖励的人的集合由包含与排斥原理,可得

(1) $|A\cap C|=|A|+|C|-|A\cup C|\ge 93+70-100=63$,

所以,受过奖励的团员至少占63%.

(2) $|A\cap B\cap C|=|A|+|B|+|C|-|A\cup B|-|B\cup C|-|A\cup C|+|A\cup B\cup C|$,

因为 $-|A\cup C|+|A\cup B\cup C|\ge 0$,所以

$|A\cap B\cap C|\ge|A|+|B|+|C|-|A\cup B|-|B\cup C|\ge 93+80+70-100-100=43$,

故三者兼而有之的人至少占43%.

3.求不大于1000的正整数中

(1)不能被5,6,8中任何一个整数整除的个数.

(2)既非平方数也非立方数的个数.

解 利用包含与排斥原理.

设 X 为不大于1000的正整数集合,A 为不能被5整除的正整数集合,B 为不能被6整除的正整数集合,C 为不能被8整除的正整数集合.则

$|A|=\frac{1000}{5}=200,\quad |B|=\left\lfloor\frac{1000}{6}\right\rfloor=166,\quad |C|=\left\lfloor\frac{1000}{8}\right\rfloor=125.$

并可求出 $|A\cap B|=\left\lfloor\frac{1000}{5\times 6}\right\rfloor=33,\quad |B\cap C|=\left\lfloor\frac{1000}{[6,8]}\right\rfloor=41,\quad |A\cap C|=\left\lfloor\frac{1000}{5\times 8}\right\rfloor=25,$

$|A\cap B\cap C|=\left\lfloor\frac{1000}{[5,6,8]}\right\rfloor=8,$ 其中[6,8]和[5,6,8]为最小公倍数记号.于是得到所求的个数为

$1000-|A\cup B\cup C|=1000-|A|-|B|-|C|+|A\cap B|+|B\cap C|+|A\cap C|-|A\cap B\cap C|$

$=1000-200-166-125+33+41+25-8=600.$

(2)设 A 为 X 中非平方数的集合,B 为 X 中非立方数的个数则

$|A|=\left\lfloor\sqrt{1000}\right\rfloor=31,\quad |B|=\left\lfloor\sqrt[3]{1000}\right\rfloor=10,\quad |A\cap B|=\left\lfloor\sqrt[6]{1000}\right\rfloor=3.$

故得所求的个数为

$1000-|A\cup B|=1000-31-10+3=962.$

4. 设 $|A|=m,|B|=n$,求

(1) A 到 B 的单射有多少个?

(2)当 $m=3,n=2$ 时,A 到 B 的满射有多少个?(对一般情形,求满射数的问题可参看[6]p.52－53).

解 (1)显然,当 $m>n$ 时,不存在 A 到 B 的单射.当 $m\le n$ 时,A 到 B 的单射的个数等于选排列数:

$P_n^m=n(n-1)\cdots(n-m+1).$

(2)求满射的个数的问题在<组合数学>里讨论,如未学组合数学,目前只能用枚举法.不难列出所有的满射为

$f_1=\begin{pmatrix}a_1&a_2&a_3\\b_1&b_1&b_2\end{pmatrix},\quad f_2=\begin{pmatrix}a_1&a_2&a_3\\b_1&b_2&b_1\end{pmatrix},\quad f_3=\begin{pmatrix}a_1&a_2&a_3\\b_2&b_1&b_1\end{pmatrix},\quad f_4=\begin{pmatrix}a_1&a_2&a_3\\b_2&b_2&b_1\end{pmatrix},$

$f_5=\begin{pmatrix}a_1&a_2&a_3\\b_2&b_1&b_2\end{pmatrix},\quad f_6=\begin{pmatrix}a_1&a_2&a_3\\b_1&b_2&b_2\end{pmatrix}.$

故共有6个.

5. 证明(0,1)与 $(-\infty,+\infty)$ 等势.

证 作映射 $f:x\mapsto\ln\frac{x}{1-x}$.

可证 f 是单射:任取 $x_1,x_2\in(0,1)$,由

$\ln\frac{x_1}{1-x_1}=\ln\frac{x_2}{1-x_2}\Rightarrow\frac{x_1}{1-x_1}=\frac{x_2}{1-x_2}\Rightarrow x_1-x_1x_2=x_2-x_1x_2\Rightarrow x_1=x_2,$

所以 f 是单射.

再证 f 是满射:任取 $y\in(-\infty,+\infty)$,令 $y=\ln\frac{x}{1-x}$,可解出 $x=\frac{e^y}{1+e^y}\in(0,1)$,使 $f(x)=y$,故 f 是满射.

综上,f 是双射,因此(0,1)与 $(-\infty,+\infty)$ 等势.

6. $f:A\to B,\ S\subseteq A$,举例说明 $f^{-1}[f(S)]=S$ 是否成立?

解 不一定成立.(注意符号的意义.)

先看一个反例.例如,$f:x\mapsto x^2\,(R\to R)$,

取 $S=\{1,2\}$,则 $f(S)=\{1,4\}$,但 $f^{-1}[f(S)]=\{\pm1,\pm2\}\ne S$.

一般的规律是当 f 是单射时,$f^{-1}[f(S)]=S$ 成立.

证明如下:

因为 f 是单射,$\forall x\in S$,如 $f(x)=a$,则 a 的原像 x 是唯一的,因而 $f^{-1}[f(x)]=x$,所以 $f^{-1}[f(S)]=S$.

7 设$|A| < \infty$, $f: A \to A$, 证明以下三个命题等价:
(1) f是单射;
(2) f是满射;
(3) f是双射.

证 用循环证法.
(1) $\Rightarrow$ (2): 因为f是单射, 且A有限, 故有$|f(A)| = |A|$, 所以f是满射.
(2) $\Rightarrow$ (3): 因为f是是满射, 故有$f(A) = A$.不妨设令$A = \{1,2,\cdots,n\}$,
$f = \begin{pmatrix} 12\cdots n \\ i_1 i_2 \cdots i_n \end{pmatrix}$, 可得$\{i_1, i_2, \cdots, i_n\} = A$.
所以$i_1, i_2, \cdots, i_n$互不相同, f是单射.
(3) $\Rightarrow$ (1): 显然.

8. 设$A \neq \varnothing$, 证明不存在A到A的幂集$\mathrm{P}(A)$的双射.

证 用反证法.
假设存在A到A的幂集$\mathrm{P}(A)$的双射$f: a \mapsto f(a) = S_a \in \mathrm{P}(A)$.
取子集 $T = \{x \in A | x \notin S_x\}$, 显然$T \subset A$或$T = \varnothing$, 因而$T \in \mathrm{P}(A)$.
由于f是双射, 且$A \neq \varnothing$, 必有$b \in A$使$f(b) = S_b = T$.则
当$b \in T$时有$b \notin S_b = T$, 矛盾;
当$b \notin T$时有$b \in S_b = T$, 矛盾.
得证.

习题 1.3

1. $A = \{1,2,3,4,5\}$, 在2^A中定义$\sim$: $S \sim T \Leftrightarrow |S| = |T|$.
证明$\sim$是等价关系, 写出等价类和商集.

证 易证$\sim$满足等价关系的三个条件.(略)
等价类为: $\overline{\varnothing} = \{\varnothing\}$, $\overline{\{1\}} = \{\{1\},\{2\},\{3\},\{4\},\{5\}\}$,
$\overline{\{1,2\}} = \{\{1,2\},\{1,3\},\{1,3\},\{1,4\},\{1,5\},\{2,3\},\{2,4\},\{2,5\},\{3,4\},\{3,5\},\{4,5\}\}$,
$\overline{\{1,2,3\}} = \{\{1,2,3\},\{1,2,4\},\cdots,\{3,4,5\}\}$,
$\overline{\{1,2,3,4\}} = \{\{1,2,3,4\},\cdots,\{2,3,4,5\}\}$,
$\overline{A} = A$.
商集为 $2^A/\sim = \{\overline{\varnothing}, \overline{\{1\}}, \overline{\{1,2\}}, \overline{\{1,2,3\}}, \overline{\{1,2,3,4\}}, \overline{A}\}$

2. $S = \{0,1,\cdots,n\}$, $f: A \mapsto$ 秩(A) $(M_n(R) \to S)$,
求f所决定的等价关系, 等价类和商集.

解 f所决定的等价关系$\sim$为: $A \sim B \Leftrightarrow$ 秩(A) = 秩(B).
等价类为 $\overline{\begin{bmatrix} I_k & 0 \\ 0 & 0 \end{bmatrix}} = \{A \in M_n(R) | \text{秩}(A) = k\}$, $k = 0,1,\cdots,n$.
商集为 $M_n(R)/\sim = \left\{\overline{\begin{bmatrix} I_k & 0 \\ 0 & 0 \end{bmatrix}} \middle| k = 0,1,\cdots,n\right\}$

3. 在$M_n(C)$中定义二元关系$\sim$: $A \sim B \Leftrightarrow \exists P$使$P^{-1}AP = B$,
证明$\sim$是等价关系, 并选等价类的代表元最简单.

证 易证$\sim$满足等价关系的三个条件.(略)
等价类的代表元可选约当标准形矩阵.

4. S为n阶实对称矩阵的集合, 定义$\sim$: $A \sim B \Leftrightarrow \exists$可逆阵使$P^T AP = B$.
证明$\sim$是等价关系, 并求$|S/\sim|$.

证 易证$\sim$满足等价关系的三个条件.(略)
由于 $S/\sim = \left\{\overline{\begin{bmatrix} -I_k & 0 & 0 \\ 0 & I_l & 0 \\ 0 & 0 & 0 \end{bmatrix}} \middle| 0 \le k + l \le n\right\}$,
所以 $|S/\sim| = \sum_{m=0}^{n}(m+1) = \frac{(n+1)(n+2)}{2}$.

5. 举一个偏序集但不是全序集的例子，并画图。
解 考虑到画图的方便，可举有限集的例子，例如：有限集的幂集对包含关系所构成的偏序集，有限整数集对整除关系所构成的偏序集。
详解略。

6. 已知两个偏序集的图形, 分别写出偏序集的偏序关系.

解 按偏序的定义, 可直接列出有偏序关系的元素对.
(a)的偏序集可表为$(S, \le)$, 其中
$S = \{a,b,c,d,e,f,g\}$, $\le = \{a < b, a < c, b < d, b < e, c < f, c < g\}$.
(b)的偏序集可表为$(T, \le)$, 其中
$T = \{a,b,c,d,e,f\}$, $\le = \{a < b, a < c, b < d, b < e, d < f, e < f\}$.

7. 用两种方法定义Z的序, 使它成为一个良序集.

解 除了普通序外我们可重新定义序, 首先要使整个集合有最小元, 例如,
(1)定义Z中的偏序关系$\le$为:
$a < b \Leftrightarrow |a| < |b|$ 或 $|a| = |b|$且$a < b$,
$a = b \Leftrightarrow a = b$.
其中右端的$<, =$为普通的序关系.
按此序排列的整数集合为:
$0, -1, 1, -2, 2, -3, 3, \cdots\cdots$.
下证它是良序集: 首先显然他它是全序集, 其次证明它的任一子集都有最小元:
设S是$(Z, \le)$的任一非空子集, 任取$a \in S$, 由于在$(Z, \le)$中$\le a$的元素为有限个, 故在S中$\le a$的元素也为有限个, 可找到最小元, 此最小元也是S的最小元.
所以$(Z, \le)$是良序集.
(2)(1)定义Z中的偏序关系$\le$为:
$a < b \Leftrightarrow |a-1| < |b-1|$ 或 $|a-1| = |b-1|$且$a < b$,
$a = b \Leftrightarrow a = b$.
其中右端的$<, =$为普通的序关系.
按此序排列的整数集合为:
$1, 0, 2, -1, 3, -2, 4, -3, 5, \cdots\cdots$.
类似可证$(Z, \le)$是良序集.

习题 1.4

1. a=493, b=391, 求(a,b), [a,b] 和 p, q。
解 方法一、辗转相除法。列以下算式：
a=b+102
b=3×102+85
102=1×85+17
由此得到 (a,b)=17, [a,b]=a×b/17=11339。
然后回代：17=102-85=102-(b-3×102)=4×102-b=4×(a-b)-b=4a-5b.
所以 p=4, q=-5.
方法二、大衍求一术。
公式与计算表格如下：

k	qk	rk	ck	dk
-1		a=493	1	0
0		b=391	0	1
1	1	102	1	1
2	3	85	3	4
3(n)	1	17	4	5
4(n+1)	5	0		

由此求得 n=3

d=(a,b)=17,

p=(-1)n-1cn=4, q=(-1)ndn=-5。

2. 求 n=504 的标准分解式和φ(n).

解 $504=2^3\times3^2\times7$.

φ(504)=504(1-1/2)(1-1/3)(1-1/7)=144.

3. 一队伍成 10 行、15 行、18 行、24 行均成方形，问需要多少人？

解 求最小公倍数：作以下算式

5 | 10, 15, 18, 24

2 | 2 3 18 24

3 | 1 3 9 12

1 1 3 4

得 [10，15，18，24]=5×2×3×3×4=360。

所以需要 360k(k>0) 人。

4. 方程 ax+by=c 在整数范围内有解的充分必要条件是 (a,b)|c 。

证 必要性：由于 (a,b)|a, (a,b)|b，所以 (a,b)|ax+by=c 。

充分性：设 d=(a,b), 于是存在整数 p, q 使 pa+qb=d 。

又由 d|c ，可设 c=dh 。因而有 aph+bqh=dh=c 。

所以 x=ph , y=qh 就是一个解。

5. 分别解同余方程：（1）258x≡131(mod348). (2) 56x=88(mod96).

解 由书中解同余方程的四个步骤求解。

（1）求 (a,m)=(258,348)=6,

6 不能整除 131，所以此同余方程无解。

（2）求 (a,m)=(56,96)=8，由于 8 能整除 88，所以此同余方程有解。

$a_1=56/8=7$, $b_1=88/8=11$, $m_1=96/8=12$.

用辗转相除法求 p,q 满足 p a_1+q m_1=1，得 p=-5。

所以方程的解为 x≡pb_1 (mod m_1) ≡-5×11(mod12) ≡ 5(mod12)。

或 x=5+12k(k 为任意整数)。

6. 解同余方程组：

x≡3(mod5)

x≡7(mod9)

解 按解同余方程组的三个步骤：

首先，计算 M=5×9=45, M_1=9, M_2=5.

其次，解两个一次同余式，由于这两个同余式有其特殊性：右端都是 1，且(a,m)=1。因而

有时可用观察法得到 pa+qm=1,从而得到 p。

1) 9x≡1(mod5),

观察得到 -9+2×5=1, p=-1.

所以此一次同余式的一个特解为 c=-1≡4(mod5).

2)5x≡1(mod9),

观察得到 2×5-9=1, p=2.

所以此一次同余式的一个特解为 c=2(mod9).

最后，将得到的一次同余式的一个特解代入公式，得到同余方程组的解：

$x=b_1c_1M_1+b_2c_2M_2$=3×4×9+2×7×5(mod45)=43(mod45)。

7. 5 行多 1，6 行多 5，7 行多 4，11 行多 10，求兵数。

解 设兵数为 x，则 x 满足以下同余方程组：

x=1(mod5)

x=5(mod6)

x=4(mod7)

x=10(mod11)

按解同余方程组的步骤，计算如下：

M=5×6×7×11=2310, M_1=462, M_2=385, M_3=330, M_4=210.

分别解以下一次同余式：

462x=1(mod5)，得 c_1=3.

385x=1(mod6)，得 c_2=1.

330x=1(mod7)，得 c_3=1.

210x=1(mod11)，得 c_4=1.

代入同余方程组的解的公式，得

x=1×3×462+5×1×385+4×1×330+10×1×210(mod2310)

=2111(mod2310).

由实际问题的意义，x 应取正数，所以兵数为

x=2111+2310k(k 非负整数)。

第二章

习题 2.1

1. 设$G=\{A=(a_{ij})_{n\times n} \mid a_{ij}\in Z, \det A=1\}$,证明$G$对矩阵乘法构成群.

证 要证满足封闭性,结合律,单位元,逆元.

封闭性：$\forall A,B\in G$, $\det(AB)=(\det A)(\det B)=1$,所以$AB\in G$.

结合律：矩阵乘法满足结合律.

单位元：单位矩阵I, $\det I=1$,所以$I\in G$.

逆元：$\forall A\in G$, $A^{-1}=\frac{1}{\det A}A^*=A^*$, A的伴随矩阵A^*的元素仍为整数,且 $\det(A^{-1})=(\det A)^{-1}=1$所以$A^{-1}\in G$.

因而G是群.

2. $Q=\{\pm E,\pm I,\pm J,\pm K\}$, $E=\begin{bmatrix}1&0\\0&1\end{bmatrix}$, $I=\begin{bmatrix}0&-1\\1&0\end{bmatrix}$, $J=\begin{bmatrix}i&0\\0&-i\end{bmatrix}$, $K=\begin{bmatrix}0&i\\i&0\end{bmatrix}$.

证明Q对矩阵乘法构成群.

证 封闭性：易证 $I^2=J^2=K^2=-E$,

$IJ=K=-JI$, $JK=I=-KJ$, $KI=J=-IK$.所以封闭性成立.

结合律：矩阵乘法满足结合律.

单位元：E.

逆元：$I^{-1}=-I, J^{-1}=-J, K^{-1}=-K$.均在$Q$中.

所以Q是群.

3. 设$G=\left\{f(x)=\frac{ax+b}{cx+d} \middle| a,b,c,d\in R, \begin{vmatrix}a&b\\c&d\end{vmatrix}=1\right\}$,

证明G关于变换的复合构成群.

证 封闭性：任取$f_1(x)=\frac{a_1x+b_1}{c\ \ x+d_1}$, $f_2(x)=\frac{a_2x+b_2}{c_2x+d_2}$,通过计算可得

$f_3(x)=\frac{a_3x+b_3}{c_3x+d_3}$,其中$\begin{bmatrix}a_3&b_3\\c_3&d_3\end{bmatrix}=\begin{bmatrix}a_1&b_1\\c_1&d_1\end{bmatrix}\begin{bmatrix}a_2&b_2\\c_2&d_2\end{bmatrix}$,

由于$\begin{vmatrix}a_3&b_3\\c_3&d_3\end{vmatrix}=\begin{vmatrix}a_1&b_1\\c_1&d_1\end{vmatrix}\begin{vmatrix}a_2&b_2\\c_2&d_2\end{vmatrix}=1$,所以$f_3=f_1f_2\in G$.

结合律：变换的复合满足结合律.

单位元：单位元为$e(x)=x=\frac{1\cdot x+0}{0\cdot x+1}\in G$.

逆元：任取$f(x)=\frac{ax+b}{cx+d}\in G$,则$f(x)$的逆元为

$f^{-1}(x)=\frac{a'x+b'}{c'x+d'}$,其中$\begin{bmatrix}a'&b'\\c'&d'\end{bmatrix}=\begin{bmatrix}a&b\\c&d\end{bmatrix}^{-1}$.

综上,G是群.

4. 举例说明，把定理 3 中条件 S3’改为：对任意 a 有右逆元 aR-1：

a aR-1=eL ，则定理不成立。

证 只需举一反例。

设 G={a,b}，乘法表如下：

×	a	b
a	a	b
b	a	b

可验证满足结合律，故（G,×）是半群；

左单位元为 a；

右逆元：aR-1=a，bR-1=a 。

但无单位元，所以 G 不是群。

5. M 为含幺半群，证明 $b=a^{-1}$ 的充分必要条件是 aba=a 和 ab2a=e。

证 必要性：将 b 代入即可得。

充分性：利用结合律作以下运算：

ab=ab(ab2a)=(aba)b2a=ab2a=e，

ba=(ab2a)ba=ab2 (aba)=ab2a=e，

所以 $b=a^{-1}$。

6. 列出 S3 的乘法表。

解 参看例 8。练习置换的乘法。

作以下乘法表，注意乘法的左右次序。

•	σ1	σ2	σ3	σ4	σ5	σ6
σ1	σ1	σ2	σ3	σ4	σ5	σ6
σ2	σ2	σ1	σ5	σ6	σ3	σ4
σ3	σ3	σ6	σ1	σ5	σ4	σ2
σ4	σ4	σ5	σ6	σ1	σ2	σ3
σ5	σ5	σ4	σ2	σ3	σ6	σ1
σ6	σ6	σ3	σ4	σ2	σ1	σ5

7. 有限代数系（G，•）中有单位元 1，则 G 为群的充分必要条件是

（1）乘法表中每行每列包含每一个元素；

（2）对 G 中任意两个元素 x, y，在乘法表中任一个以 1, x, y 为顶点的长方形上的第四个顶点的元素只依赖于 x, y ，而与 1 的选择无关。

证 由于 G 有有限个元素，可设 G={a1,a2,...,an}。可以想象，可作出一个乘法表，表头上面和左边为这 n 个元素：a1,a2,...,an。先证必要性。

必要性：(1) 由乘法表的规律，第 i 行的元素为：aia1, aia2,..., aian 。由 aia1=aia2 和消去律，得 a1=a2，矛盾。因而 aia1≠aia2。所以第 i 行的元素互不相同。从而有{ aia1, aia2,..., aian}=G，

即第 i 行包含 G 的每一个元素。

（2）在乘法表中任取一个 1，在同一列中必有一个 x，在同一行中必有一个 y，设第四个顶点的元素为 z，见下图，

&#0;	..........a-1........................c..................
...... a ...... b	....1..........................y................. ....x..........................z................. ....

则有

x=ba-1, y=ac,

所以

z=bc=xy。与 1 的选择无关。

充分性：封闭性：由乘法表保证。

在证明结合律之前，我们由乘法表的性质（1）、(2)，对于乘法表中以 1、x、y、z 为顶点的长方形，必有

z=xy。下证结合律。

结合律：任取 x，y，z。要证 (xy)z=x(yz).

在乘法表中任取一个 1，在同一列中必有一个 x，在同一行中必有一个 y，则第四个顶点的元素为 xy。在 y 的同一列中必有一个 1，与这个 1 同一行中必有一个 z，见下图，

&#0;	....
....	....1..........................y................yz....... ....x..........................xy...............w........ ....1............... z......... ....

我们来看元素 w 的值：

对以 1、x、yz、w 为顶点的长方形，有 w=x(yz),

对以 1、xy、z、w 为顶点的长方形，有 w=(xy)z,

所以 (xy)z=x(yz)，即结合律成立。

单位元：题设。

逆元：由（1）保证。

习题 2.2

1.举例：半群有单位元,而子半群无单位元或有不同的单位元.

例 可从矩阵半群中找.

设 $G=\left\{\begin{bmatrix}0&0\\0&0\end{bmatrix},\begin{bmatrix}1&0\\0&1\end{bmatrix},\begin{bmatrix}1&0\\0&0\end{bmatrix},\begin{bmatrix}0&1\\0&0\end{bmatrix}\right\}$,不难验证它是半群,单位元为$\begin{bmatrix}1&0\\0&1\end{bmatrix}$.

$H=\left\{\begin{bmatrix}0&0\\0&0\end{bmatrix},\begin{bmatrix}1&0\\0&0\end{bmatrix}\right\}$,不难验证它也是半群,而单位元为$\begin{bmatrix}1&0\\0&0\end{bmatrix}$.

$N=\left\{\begin{bmatrix}0&0\\0&0\end{bmatrix},\begin{bmatrix}1&0\\0&0\end{bmatrix},\begin{bmatrix}0&1\\0&0\end{bmatrix}\right\}$不难验证它也是半群,但无单位元.

2. H 是 G 的有限子集，证明 H 是子群的充分必要条件是对任意

$a,b\in H$ 有 $ab\in H$。

证 必要性：显然。

充分性：由于封闭性成立，H 是半群。又因群 G 中消去律成立，故 H 中消去律也成立。由 2.1 节定理 5，知 H 是群。

3. 找出 Z 和 Z_{12} 中全部子群。

解 Z 中全部子群：$H_m=\{mk|k\in Z\}$, m=0,1,2,......。

Z_{12} 中全部子群：$N_0=\{0\}$，$N_1=\{0，2，...，10\}$，$N_2=\{0，3，6，9\}$，$N_3=\{0，4，8\}$，

$N_4=\{0，6\}$，$N_5= Z_{12}$ 。

4. 设 G 是群，证明对任意 a,b 有 $o(ab)=o(ba)$。

证 设 $o(ab)=n$，则 $(ab)^n=e$，$a(ba)^{n-1}b=e$，即 $(ba)^{n-1} =a^{-1}b^{-1}$，

故得 $(ba)^n=e$，所以 $o(ba)|n$，即 $o(ba)|o(ab)$。

类似可证 $o(ab)|o(ba)$。

综上，$o(ab)=o(ba)$。

5. 设 G 是群，$|G|=2n$，则 G 中有 2 阶元。

证 利用任何元素 a 与它的逆元的关系。

对任何非单位元 a 有：$a=a^{-1}$ 的充分必要条件是 $o(a)=2$。因而对于阶数大于 2 的元素总是成对出现的，即阶数大于 2 的元素的个数是偶数，所以，除单位元之外至少有 1 个 2 阶元。

6. 设 G 是群，若任意 a,b 有 $(ab)^2=a^2b^2$，则 G 是 Abel 群。

证 利用群内元素的运算关系。

把 $(ab)^2=a^2b^2$ 写成 abab=aabb，由消去律得

ba=ab。

所以 G 是 Abel 群。

7. 设 G 是非 Abel 群，证明存在非单位元 a,b，$a\neq b$ 使 ab=ba。

证 利用元素和它的逆可交换，或元素和它的幂可交换。但要求元素和它的逆（幂）不等。

由于 G 是非 Abel 群，必有阶数大于 2 的元素 a，因而 $a\neq a^{-1}$，取 $b= a^{-1}$，则 ab=ba。

（也可用幂来做。）

8. $o(a)=n$，$m\in Z^+$ ，则 $o(a^m)=n/(m,n)$ 。

证 要证两个整数相等，通常用互相整除的方法。

设 $o(a^m)=k$ ， $(m,n)=d$ ，

令 m=rd ， n=sd ， n/(m,n)=s ，

下证 k 与 s 互相可整除：

$(a^m)^s=a^{ms}=a^{nr}=e$ ，所以 k|s 。

另一方面，

$(a^m)^k=a^{mk}=e$ ，所以 n|mk ，得 s|rk ，由于 (r,s)=1 故 s|k 。

综上，k=s 。证毕。

9. 设 $A=(a_{ij})_{3\times 3}\in SO_3$，$A=\sigma(\eta,\theta)$，则

（1） η 可由 A-I 中两线性无关的行向量作叉积得到。

（2） θ 满足 $2\cos\theta+1=trA$ 。

证 首先要复习一下 SO_3 的意义。可从两个角度来看它的意义：从线性变换的角度，SO_3 是三维线性空间中全体旋转变换所构成的群；从矩阵角度来看，SO_3 是全体行列式为 1 的三阶正交矩阵所构成的群。因而 SO_3 中任何一个元素既可用矩阵 A 来表示，也可用旋转变换 $\sigma(\eta,\theta)$ 来表示。本题就是要讨论它们之间的关系。给定一个 A，如何来确定它所对应的旋转变换 $\sigma(\eta,\theta)$ 的旋转轴 η 和旋转角 θ 呢？旋转轴 η 就是三维空间中的一个向量，旋转角 θ 就是按右手法则转过的角度。设 $A\neq I$，则向量 η（不计正负方向和大小）和 θ 由 A 唯一确定。确定的方法如下：向量 η 的特点是在 A 的作用下不变，故满足 $A\eta=\eta$ ，即

$(A-I)\eta=0$ (*)

由于 A 的行列式为 1 的正交矩阵，1 必是 A 的一个特征值（为什么？），所以方程(*)必有非 0 解，旋转轴 η 就是 1 所对应的特征向量。下证秩(A-I)=3：首先， 秩(A-I)<3，如果 秩(A-I)=1，则 λ=1 的几何重度为 2，因而 λ=1 的代数重度大于或等于 2，令

$|\lambda I-A|=(\lambda-1)^2(\lambda-\lambda_3)$,

由|A|=1 得 $\lambda_3=1$，由 A 的正交性，得 A=I，矛盾。故秩(A-I)=2。

由方程(*)可见，η 与 A-I 的行向量正交，而 A-I 中恰有两个线性无关的行向量，所以用这两个线性无关的行向量作叉积就得到 η。

（2）设 η 为旋转轴，将 η 扩大为一组标准正交基：$\varepsilon_1=\eta/|\eta|$，$\varepsilon_2$，$\varepsilon_3$。则旋转变换 $\sigma(\eta,\theta)$ 在此组基下的矩阵为

$$B=\begin{bmatrix}1 & 0 & 0\\ 0 & \cos\theta & -\sin\theta\\ 0 & \sin\theta & \cos\theta\end{bmatrix},$$

由于 A 与 B 相似，它们有相同的迹，所以 $trA=1+2\cos\theta$ 。

习题 2.3

1. $G=\langle a,b|o(a)=n,o(b)=2,ba=a^{-1}b\rangle$,

证明 $G\cong D_n(n\geq 2)$.

证 首先我们要掌握生成群的意义：生成群是由生成元们和它们的逆所作成的一切可能的的积所构成的集合.

对于我们要研究的 G 来说，它的元素可以简化.由于 G 由 a,b 两个元素生成，G 的任意一个元素是有限个 a 与 b 和它们的逆的乘积.利用规则 $ba=b^{-1}a$，可把着个乘积中的 a 的幂统统移到前面，于是变成 a 的幂 b 和 a 的幂的乘积，再利用 a 与 b 阶可把 G 表为以下形式：

$G=\{a^ib^j|i=0,1,\cdots,n-1;j=0,1\}$

并且有 $|G|=2n$.

再复习一下二面体群的几何定义(见2.1节例9)：

$D_n=\{\rho_k,\pi_k|k=0,1,\cdots,n-1\}$

为了找到 D_n 与 G 的关系，我们把 D_n 也表为生成群的形式，由于 $\rho_k=\rho_1^k$, $\pi_k=\rho_k\pi_0=\rho_1^k\pi_0$，故得

$D_n=\{\rho_1^i\pi_0^j|i=0,1,\cdots,n-1;j=0,1\}$

现在可以来证明它们同构了.

作映射 $f:a^ib^j\mapsto\rho_1^i\pi_0^j(G\to D_n)$,

可证 f 是双射(略)，且保持运算(略).

所以 $G\cong D_n$.

2. 求 D_n 的所有最小生成元集。

解 最小生成元集指元素个数最少。首先易见 D_n 的最小生成元集所含元素个数必为 2。因而有以下两种情形：

（1）$D_n=<\rho_k,\pi_m>$。我们来看对 k 与 m 有什么条件？

由于 $\rho_1\in D_n$ ，必有 q 使 $(\rho_k)^q=\rho_1$ ，即 $\rho_{kq}=\rho_1$ <=> kq=1(mod n) <=> (k, n)=1。

所以这类最小生成元集为

$D_n=<\rho_k,\pi_m>$，(k, n)=1，m=0,1,...,n-1 。

（2）$D_n=<\pi_k,\pi_m>$。我们来看对 k 与 m 有什么条件？

方法类似。

由于 $\rho_1\in D_n$ ，必有 p，q 使 $(\pi_k)^p(\pi_m)^q=\rho_1$ ，但因 $o(\pi_i)=2$，故有

$\pi_k\pi_m=\rho_1$ <=> k-m=1(mod n) <=> (k-m, n)=1。(其中用到运算规律 $\pi_k\pi_m=\rho_{k-m}$)。

所以这类最小生成元集为

$D_n = \langle \pi_k, \pi_m \rangle$，(k-m, n)=1，k, m∈[0,n-1] 。

3. 证明 $K_4 \cong (Z_{12}^*$, &#0;)。

证 首先应搞清 K_4 和 Z_{12}^* 的意义，并写出它们的元素。

K_4={e, a, b, c}，Z_{12}^*={1,5,7,11}。

作映射 f:e→1, a→5, b→7, c→11 .

可以一一验证（略）满足

f(xy)=f(x)f(y).

所以 $K_4 \cong (Z_{12}^*$, &#0;)。

4. (Q^+, ×)和(Q, +)是否同构？

答 否！（如果把 Q 换成 R 不难证明它们是同构的。）

证明如下：

反证法：假设有同构 f: (Q, +)→(Q^+, ×).

设 f(a)=2，则

f(a)=f(a/2+a/2)=f(a/2)f(a/2)=2,

由此得

$f(a/2)=\sqrt{2}\notin Q^+$，矛盾。

所以不存在(Q, +) 到(Q^+, ×)的同构，因而(Q^+, ×)和(Q, +)不同构。

5. G=<a>为无限循环群，A=$\langle a^s \rangle$，B=$\langle a^t \rangle$，证明

（1）A∩B=$\langle a^m \rangle$, m=[s,t].

（2）<A,B>=$\langle a^d \rangle$, d=(s,t).

证 因为无限循环群都同构于(Z, +)，故问题变为：

A=<s>，B=<t>，证明(1) A∩B=<m>, m=[s,t]. (2) <A,B>=<d>, d=(s,t).

用互相包含的方法证明此二等式。

（1）任取 x∈A∩B，则 x=ps=qt，x 是 s 与 t 的公倍数，故 m|x，x∈<m>，

所以 A∩B≤<m>。

反之，显然有 m∈A 和 m∈B，因此 m∈A∩B，

所以 <m>≤A∩B。

综上，得 A∩B=<m>。

（2）任取 x∈<A,B>，则 x 可表为 x=ps+qt，因而 d|(ps+st)=x，x∈<d>，

所以 <A,B>≤<d>。

反之，由最大公因子定理，存在 a,b 使 d=as+bt，因而 d∈<A,B>，

所以 <d>≤<A,B>。

综上，得 <A,B>=<d>。

6. $G=\left\{\begin{bmatrix}1 & n\\ 0 & \pm 1\end{bmatrix} \middle| n\in Z\right\}, A=\begin{bmatrix}1 & 1\\ 0 & -1\end{bmatrix}, B=\begin{bmatrix}1 & 2\\ 0 & -1\end{bmatrix},$

证明 $G=\langle A,B\rangle$

证 方法类似于本节例1, 但更简单.

显然有 $\langle A,B\rangle\subseteq G$.

反之, 任取 $X=\begin{bmatrix}1 & n\\ 0 & 1\end{bmatrix}, Y=\begin{bmatrix}1 & n\\ 0 & -1\end{bmatrix}\in G,$

令 $C=AB=\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}$, 则 $X=\begin{bmatrix}1 & n\\ 0 & 1\end{bmatrix}=C^n, Y=\begin{bmatrix}1 & n\\ 0 & -1\end{bmatrix}=AC^{n-1},$

所以 $X,Y\in\langle A,B\rangle, G\subseteq\langle A,B\rangle$.

综上, 得证.

7. 确定无限循环群的全部极大子群。

解 首先应复习极大子群的概念：若子群 M 满足：（1）M≠G；（2）对任何 H：M<H≤G，都有 H=G。

其次，无限循环群都同构于 G=(Z,+)，而它的全部子群已知道，它的全部子群为：

<n>，n=0,1,2,...。

只要把其中的极大子群找出来就行了。

怎样从中找出极大子群呢？有若干种思路，下面介绍几种方法：

方法一、从极大子群的定义入手。

设 M=<m>，m∈Z^+，为一个极大子群，则 M≠G 和 m≠1。可取 b∈G\M，令 H=<M,b>。

显然 H>M，由极大子群的定义，得 <M, b>=G，故存在 p, q∈Z，使

pm+qb=1，

由此得 (m,b)=1，而 b 可取 1,...,m-1。即 m 与 1,...,m-1 都互素，因此 m 是素数。

所以 G 的全部极大子群为：

<p>，p 为素数。

方法二、通过简单的分析：当 n 是合数时，<n>不是极大子群，因而可猜想：当 n 是素数时，<n> 是极大子群。证明如下：

设 p 为素数，若有子群 H 满足：<p><H≤G，设 H=<n>，则由(p,n)=1 ，存在 r,s 使

rp+sn=1，因而得 1∈H, 从而 H=G。所以<p>是极大子群。

故 G 的全部极大子群为：

<p>，p 为素数。

8. 设 p 为素数，G={x|x∈C, x^{p^n}=1, n=1,2,...}，证明

G 的任何真子群是有限循环群。

证 G 是由所有 p^n 次单位根形成的群。但对于固定的 n 由所有 p^n 次单位根形成的群是有限的，因而只要证明任何一个真子群必是某个 n 的所有 p^n 次单位根形成的群。这里还要用到

真子群的概念。

首先可把 G 表为

G={exp(2kπ/p^n)|0≤k<p^n, (k, p)=1; n=1,2,...}。

设 H 是 G 的任一真子群。

由于 H 是真子群，必有一元素 exp(2qπ/p^m)，(q,p)=1 不属于 H。由此可得

所有的元素 exp(2kπ/p^n), (k, p)=1, n≥m 都不属于 H。(为什么？)

令 K={exp(2kπ/p^n)|0≤k<p^n, (k, p)=1; n<m}。则

K=< exp(2kπ/p^{m-1})>，是 p^{m-1} 阶循环群，而 H≤K，由于循环群的子群仍是循环群，

所以 H 是有限循环群。

9. $G=\langle A,B\rangle, A=\begin{bmatrix}0&1&0&\cdots&0\\0&0&1&\cdots&0\\\cdots&\cdots&\cdots&\cdots&\cdots\\0&0&\cdots&0&1\\1&0&0&\cdots&1\end{bmatrix}, B=\begin{bmatrix}1&0&0&\cdots&0\\0&\omega&0&\cdots&0\\0&0&\omega^2&\cdots&0\\\cdots&\cdots&\cdots&\cdots&\cdots\\0&0&0&\cdots&\omega^{n-1}\end{bmatrix}$，$\omega$为$n$次单位原根.

证明$|G|=n^3$.

证 要求出G的元素个数,只要写出G的元素的一般形式,类似类似于本节习题1,将由A和B及它们的逆构成的乘积简化.为此,通常考虑将BA表为A的某个幂与B的积经过简单的计算可得

$BA=\omega^{-1}AB$,且$o(A)=o(B)=n$.

故G可表为

$G=\{\omega^i A^j B^k | i,j,k=0,1,\cdots,n-1\}$

所以$|G|=n^3$.

习题 2.4

1. 设 $\sigma=(i_1,i_2,\ldots,i_k)$，$\tau\in S_n$，则

$\tau\sigma\tau^{-1}=(\tau(i_1),\ \tau(i_2),\ldots,\ \tau(i_k))$.

证 该题主要练习置换与轮换的记号与运算。首先要把题目看懂。

要证两点：

（1）对于任何 $j\in\{\tau(i_1),\ \tau(i_2),\ldots,\ \tau(i_k)\}$ 有

$\tau\sigma\tau^{-1}(\tau(i_m))=\ \tau(i_{m+1})$.

（2）对于任何 j 不属于$\{\tau(i_1),\ \tau(i_2),\ldots,\ \tau(i_k)\}$ 有

$\tau\sigma\tau^{-1}(j)=j$.

具体运算很简单，证明如下：

（1）对于任何 $j\in\{\tau(i_1),\ \tau(i_2),\ldots,\ \tau(i_k)\}$ 有

$\tau\sigma\tau^{-1}(\tau(i_m))=\ \tau\sigma(i_m)=\ \tau(i_{m+1})$.

m=1,2,... 下标的加法为模 k 的加法。

（2）对于任何 j 不属于$\{\tau(i_1),\ \tau(i_2),\ldots,\ \tau(i_k)\}$ 有

$j=\tau(i)$, $i\neq i_1, i_2,\ldots, i_k$, 和（注意到 $\sigma(i)=i$）

$\tau\sigma\tau^{-1}(j)=\ \tau\sigma\tau^{-1}(\tau(i))=\ \tau\sigma(i)=\ \tau(i)=j$.

综上得证。

另一证法：上面的证法中利用置换的轮换形式，由于对某一置换的不动点不出现在轮换中，因而需分两种情况。如果采用置换的普通形式，则证明可简单一些。

σ 可表为 $\sigma=\begin{pmatrix}i_1&\cdots&i_2&\cdots&i_k&\cdots\\i_2&\cdots&i_3&\cdots&i_1&\cdots\end{pmatrix}$,

设 $\tau=\begin{pmatrix}i_1&\cdots&i_2&\cdots&i_k&\cdots\\j_1&\cdots&j_2&\cdots&j_k&\cdots\end{pmatrix}$,

则

$\tau\sigma\tau^{-1}=$

$\begin{pmatrix}i_1&\cdots&i_2&\cdots&i_k&\cdots\\j_1&\cdots&j_2&\cdots&j_k&\cdots\end{pmatrix}\begin{pmatrix}i_1&\cdots&i_2&\cdots&i_k&\cdots\\i_2&\cdots&i_3&\cdots&i_1&\cdots\end{pmatrix}\begin{pmatrix}j_1&\cdots&j_2&\cdots&j_k&\cdots\\i_1&\cdots&i_2&\cdots&i_k&\cdots\end{pmatrix}$

$=\begin{pmatrix}j_1&\cdots&j_2&\cdots&j_k&\cdots\\j_2&\cdots&j_3&\cdots&j_1&\cdots\end{pmatrix}=\begin{pmatrix}\tau(i_1)&\cdots&\tau(i_2)&\cdots&\tau(i_k)&\cdots\\\tau(i_2)&\cdots&\tau(i_3)&\cdots&\tau(i_1)&\cdots\end{pmatrix}$

$=(\tau(i_1)\quad\tau(i_2)\quad\cdots\quad\tau(i_k))$.

2. 证明 $|A_n|=n!/2$.

证 实际上要证 A_n 的元素个数是 S_n 的元素个数的一半，或 S_n 中偶置换的个数与奇置换的个数相等。为此我们来找偶置换的集合与奇置换的集合之间的关系。

设 B 为 S_n 中全体奇置换的集合，任取奇置换 $\sigma\in S_n$，则

σB 属于 A_n，故 $|\sigma B|\leqslant|A_n|$，即 $|B|\leqslant|A_n|$。

反之，

σA_n 属于 B，故 $|\sigma A_n|\leqslant|B|$，即$|A_n|\leqslant|B|$。

综上，得

$|A_n|=|B|=n!/2$。

所以 S_n 中奇、偶置换各半。

3. 证明任何一个置换群中，或全部元素均为偶置换，或奇、偶置换各半。

证 证明方法同上题。（略）

4. 证明 $S_n=\langle(12),(123\ldots n)\rangle$。

证 方法类似于本节例 4。注意熟悉生成群和生成元的意义、置换的乘法运算。并可利用已知的置换运算公式，例如本节习题第 1 题就是一个公式。

我们可以利用本节例 4 的结果：$S_n=\langle(12),(13),\ldots,(1n)\rangle$。只要证明 (1i) 可由 (12) (123...n) 生成。

令 $\sigma=(12)$， $\tau=(123\ldots n)$，则由本节习题第 1 题的公式得

$\tau\sigma\tau^{-1}=(23)$，$\sigma(23)\sigma^{-1}=(13)$，...

所以 $\langle\sigma,\ \tau\rangle=\langle(12),(13),\ldots,(1n)\rangle=S_n$ 。

5. 证明 $A_n=\langle(123),(124),\ldots,(12n)\rangle$ 。

证 方法类似于上题。但要利用偶置换的性质。

显然，$\langle(123),(124),\ldots,(12n)\rangle\leqslant A_n$ 。

反之，任取 $\sigma\in A_n$ ，σ 可表为

$\sigma=(1i_1)(1j_1)(1i_2)(1j_2)\ldots(1i_k)(1j_k)$，

又由 (1i)(1j)=(1ji)=(1i2)(12j)(12i) 得

$\sigma\in\langle(123),(124),\ldots,(12n)\rangle$。

所以 $A_n=\langle(123),(124),\ldots,(12n)\rangle$ 。

6. 求出正四面体的旋转群。

解 可先作一个正四面体的图，顶点为 1，2，3，4。每一个绕对称轴的旋转且保持空间位置不变的变换，对应一个四元置换。所有这样的置换构成正四面体的旋转群。

它的对称轴可分两类：

第一类为过一顶点和底面中心的轴分别旋转 120° 和 240° ，这样的旋转有：

(1)，(234)，(243)，(134)，(143)，(124)，(142)，(123)，(132)。

第一类为过两条对边的中点的轴，旋转 180° ，这样的旋转有：

(12)(34)，(13)(24)，(14)(23)。

所以正四面体的旋转群为

G={(1)，(234)，(243)，(134)，(143)，(124)，(142)，(123)，(132)，(12)(34)，(13)(24)，(14)(23)}=A_4 。

7. 证明正立方体的旋转群同构于 S_4。

证 正立方体的旋转群在本节中已求出，共有 24 个元素，与 S_4 的元素个数相同。但如何找到它们的元素之间的对应关系呢？主要的问题在于，正立方体的旋转群的基集有 8 个元素，而 S_4 的基集有 4 个元素。为此，我们可把正立方体的 8 个顶点两两一组分为 4 组，分组的原则是在旋转过程中始终在一起。例如可取以下分组方法：

令 a={1,7}，b={2,8}，c={3,5}，d={4,6}。则可把正立方体的旋转群的每一个元素变为集合{a, b, c, d}上的一个置换，例如，旋转 (1234)(5678) 就变为 (abcd) 。其余元素的变化略。

由此证明了正立方体的旋转群同构于 S_4。

8. 确定 S_n 中长度为 n 的轮换的个数。

解 S_n 中长度为 n 的轮换可表为

$(1, i_2, i_3, ..., i_n)$。

由于 $i_2, i_3, ..., i_n$ 为 2,3,...,n 的任一排列，所以 S_n 中长度为 n 的轮换的个数等于 (n-1) 阶全排列数：(n-1)! 。

习题 2.5

1. 设 H≤G，a,b∈G，证明以下命题等价：

（1）$a^{-1}b\in H$,(2)$b\in aH$,(3)$aH=bH$,(4)$aH\cap bH\neq\varnothing$。

证 本题主要熟悉陪集性质。用循环证法。

（1）=>（2）：$a^{-1}b\in H \Rightarrow a^{-1}b=h \Rightarrow b=ah \Rightarrow b\in aH$。

（2）=>（3）：$b\in aH \Rightarrow bh\in aH \Rightarrow bH$ 属于 aH，另一方面，$b\in aH \Rightarrow b=ah \Rightarrow a=bh^{-1} \Rightarrow aH$ 属于 bH，综上得 aH=bH。

（3）=>（4）：aH=bH 显然有 $aH\cap bH\neq\varnothing$。

（4）=>（1）：$aH\cap bH\neq\varnothing \Rightarrow$ 存在 $h_1,h_2\in H$ 使 $ah_1=bh_2 \Rightarrow a^{-1}b=h_1h_2^{-1} \Rightarrow a^{-1}b\in H$ 。

2. $G=\{a_1 a_2 a_3 a_4 a_5 | a_i=0$ 或 $1\}$, H={00000,10101,01011,11110},

写出 H 在 G 中的所有陪集。

解 本题目的是熟悉陪集的计算。

G 的加法运算+为二进制按位加法（不进位）。不难检验 H 确为子群。作陪集时，尽量先选简单的元素作为代表元，这样计算较为简单。本题可选含 1 的个数较少的元素作代表元。由此得 H 在 G 中的陪集为：

00000+H=H,

00001+H={00001,10100,01010,11111},

00010+H={00010,10111,01001,11100},

00100+H={00100,10001,01111,11010},

01000+H={01000,11101,00011,10110}，

10000+H={10000,00101,11011,01110},

10010+H={10010,00111,11001,01100},

11000+H={11000,01101,10011,00110}.

应检验一下是否不重不漏。

3. 确定 A_4 的全部子群。

解 对有限群，子群的阶是群的阶的因子。因此我们可以按子群的阶来找所有的子群。由于$|A_4|=12$，子群的阶只能是 1, 2, 3, 4, 6, 12。对每一个子群，利用元素的阶是群的阶的因子，可用生成元表示。

1 阶子群：{(1)}。

2 阶子群：<(12)(34)>, <(13)(24)>, <(14)(23)>。

3 阶子群：<(123)>, <(124)>, <(134)>, <(234)>。

4 阶子群：{(1), (12)(34), (13)(24), (14)(23)}。

6 阶子群：由于 A_4 中无 6 阶元，故 A_4 中无 6 阶循环子群。A_4 中的 6 阶子群只能由一个二阶元和一个三阶元生成，但任一个二阶元和任一个三阶元，例如 (12)(34) 和 (123)，易证<(12)(34), (123)>= A_4。所以 A_4 中无 6 阶子群。

12 阶子群：A_4 。

4. A, B≤G, |A|<∞, |B|<∞, (|A|,|B|)=1，证明 |AB|=|A||B|。

证 设法利用本节定理 3 的公式。只需证明 $|A\cap B|=1$。

由于 $A\cap B\leq A$ 和 $A\cap B\leq B$，故$|A\cap B|$ 能同时整除 |A| 和 |B|。

又由于(|A|,|B|)=1，所以 $|A\cap B|=1$。

因此由本节定理 3 的公式得

$|AB|=|A||B|/|A\cap B|=|A||B|$。

5. A, B≤G, $C=\langle A\cup B\rangle$，证明 $[C:A]\geq[B:A\cap B]$。

证 按题意，子群指数$[C:A]$和$[B:A\cap B]$都是有限的，但群不一定是有限的。由于子群的指数等于子群的陪集的个数，可用两个子群的陪集集合之间的映射来揭示它们的数目之间的关系。

令 $D=A\cap B$, $S=\{bD|b\in B\}$, $T=\{cA|c\in C\}$,

作对应关系 f: bD→bA (S→T),

首先我们来证明 f 是映射：$b_1D=b_2D \Rightarrow b_1^{-1}b_2\in D \Rightarrow b_1^{-1}b_2\in A \Rightarrow b_1A=b_2A$ 。

并且上面的每一步均可倒推回去，所以 f 是单射。因此 |S|≤|T|, 即

$[B:A\cap B]\leq[C:A]$。

另一方法：

虽不能直接利用本节定理 3，但可利用它的证明方法。并用 BA 作为中间集合。

首先，BA 属于 C，$[BA:A]=|\{bA|b\in B\}|$，显然有 $[BA:A]\leq[C:A]$。

其次，由定理 3 的证明过程（请查阅），可得 $[B:A\cap B]= [BA:A]$，所以 $[B:A\cap B] \leq[C:A]$。

6. A, B≤G, 若有 g,h∈G 使出 Ag=Bh, 则 A=B。

证 采用互相包含的方法来证明集合的相等。为此先将 g 和 h 表达出来。

由 Ag=Bh 可得存在 a∈A, b∈B 使 g=bh, ag=h, 从而得 $g^{-1}=h^{-1}b^{-1}$, $h^{-1}=g^{-1}a^{-1}$.

对任意 x∈A 有 $xg=b_1h$, 因而 $x= b_1hg^{-1}=b_1hh^{-1}b^{-1}= b_1b^{-1}\in B$, 故 A 属于 B。

反之，对任意 y∈B 有 $a_1g=yh$, 因而 $y=a_1gh^{-1}=a_1gg^{-1}a^{-1}=a_1a^{-1}\in A$, 故 B 属于 A。

综上，得 A=B 。

7. $A\leq B\leq G \Rightarrow [G:A]=[G:B][B:A]$

证 按题意，A, B的指数是有限的，但A, B本身不一定是有限.所以不能直接套用拉格朗日定理.但可用证明中所用陪集分解的方法.

设$[G:B]=m$, $[B:A]=n$, 则G与B可表为

$$G=\bigcup_{i=1}^{m} g_iB,\quad B=\bigcup_{j=1}^{n} b_jA,$$ 注意其中陪集的代表元已取定.

则有

$$G=\bigcup_{i=1}^{m}\bigcup_{j=1}^{n} g_ib_jA.$$

下证式中不同陪集互不相交：

由于 $g_ib_jA=g_kb_lA \Rightarrow b_j^{-1}g_i^{-1}g_kb_l\in A \Rightarrow g_i^{-1}g_k\in b_jAb_l^{-1}$

$\Rightarrow g_i^{-1}g_k\in B \Rightarrow g_i=g_k \Rightarrow i=k$

$\Rightarrow b_jA=b_lA \Rightarrow b_j=b_l \Rightarrow j=l.$

因而 $(i,j)\neq(k,l) \Leftrightarrow g_ib_jA\neq g_kb_lA \Leftrightarrow g_ib_jA\cap g_kb_lA=\varnothing.$

所以 $[G:A]=mn=[G:B][B:A]$

习题 2.6

1. $A\lhd G$，$B\lhd G$，证明：$A\cap B\lhd G, AB\lhd G$

（$\lhd$ 表示正规子群）

证明：$\forall g\in G, a\in A\cap B. gag^{-1}\in A, gag^{-1}\in B$

$\Rightarrow gag^{-1}\in A\cap B \Rightarrow A\cap B\lhd G$

由于$AB=BA$, 得$AB\lhd G$, 又$\forall g\in G$，$ab\in AB$

$gabg^{-1}=gag^{-1}\cdot gag^{-1}=a_1b_1\in AB \therefore AB\lhd G$

2. $A\lhd G, B\leq G \Rightarrow A\cap B\lhd B, AB\leq G$

证明：$\forall b\in B, a\in A\cap B, bab^{-1}\in A$，显然$bab^{-1}\in B$

$\therefore bab^{-1}\in A\cap B, A\cap B\lhd B$

$\forall ab\in AB, ab\in AB=BA. \therefore ab=ba_1\in BA, AB\subseteq BA$

类似可得$BA\subseteq AB$，故$AB=BA, AB\subseteq G$

3.$H\le G, \{aH\mid a\in G\}$关于子集乘法成群$\Rightarrow H\lhd G$

证明：

方法一：

由于$aH\cdot H=aH$，故H是单位元.

因而有$HaH=aH$，即$a^{-1}HaH=H$

故$\forall h\in H$有$a^{-1}ha\in H, H\lhd G$

方法二：

$\forall a,b\in G$，可令$(aH)(bH)=cH$，得$ab\in cH$

故得$(aH)(bH)=cH=abH$

于是有$aH\cdot a^{-1}H=H, aha^{-1}\in H, H\lhd G$

4.证明：4元数群Q的每一个子群均为正规子群.

证明$\because |Q|=8$，非平凡子群的阶为2与4

对4阶子群，由于其指数为2，故为正规

对于2阶群，只有一个，$H=<E,-E>$

显然也是正规子群.

5.$A,B\le G, C=<A\cup B>$，且$B\lhd C\Rightarrow C=AB$

证明：显然$AB\subseteq C$

反之，$\forall \mathbf{c}\in \mathbf{C}$，$\mathbf{c}$可表为$c=a^{k1}b^{l1}a^{k2}b^{l2}\ldots a^{ks}b^{ks}$

由$B\lhd C, \forall b\in B, a\in A$有$ba=ab_1$，故$c$可表为

$c=a^rb_2^t\in AB$即$C\subseteq AB$

$\therefore C=AB$

6.$\alpha_{ab}=aba^{-1}b^{-1}, K=\{\alpha_{ab}\text{的乘积}\}$

$(I)K\lhd G$

$(II)G/K$是可换群

(III)若$N\lhd G, G/N$可换，则$N\ge K$

证明：

易证$K\le G$，只需证明$\alpha_{ab}^{-1}\in K$

$(I)\forall k\in K$，k可表为$k=\alpha_{a_1b_1}\ldots\ldots\alpha_{a_kb_k}$

$\forall g\in G, g\alpha_{a_jb_j}g^{-1}=(ga_jg^{-1})(gb_jg^{-1})(ga_jg^{-1})^{-1}(gb_jg^{-1})^{-1}=\alpha_{a_j'b_j'}$

其中$a_j'=ga_jg^{-1}, b_j'=gb_jg^{-1}$

故$gkg^{-1}=\alpha_{a1b1}'\alpha_{a2b2}'\ldots\ldots\alpha_{akbk}'\in K$

$\therefore K\lhd G$

$(II)G/K=\{8K\mid g\in G\}$

由于$(g_1K)(g_2K)(g_1K)^{-1}(g_2K)^{-1}=g_1g_2g_1^{-1}g_2^{-1}K=K$

故$(g_1K)(g_2K)=(g_2K)(g_1K)$

即G/K可换

$(III)G/N=\{gN\mid g\in G\}$

可得$aba^{-1}b^{-1}\in N$

故$K=<aba^{-1}b^{-1}\mid a,b\in G>\le N$

7.一个可换群是单群，则它必是素数阶循环群.

证明：

方法一：

分以下情况讨论：

(1)$|G|=\infty$，任取$a\in G\setminus\{e\}$

若$o(a)=\infty$则$<a^2>\lhd G$，与G是单群矛盾

若$o(a)<\infty$则$<a>\lhd G$，与G是单群矛盾

(2)$|G|=n$

若n为合数，则有素数$p<n, p\mid n$，因而G中有p阶元a，$<a>\lhd G$

与G为单群矛盾.

故$|G|=p$(素数)，因而取$a\in G\setminus\{e\}, o(a)=p$

$G=<a>\cong(Z_p,+)$

方法二：(从元素考虑)

任取$a\in G\setminus\{e\}$

若$<a>\ne G$则$<a>\lhd G$，与G是单群矛盾

故必有$G=<a>$

(1)若$o(a)=\infty$，则$<a^2>\lhd G$，矛盾

(2)若$o(a)=$合数，则有素数$p\mid o(a), p<o(a), a^p>\lhd G$矛盾

故$o(a)=p$(素数)，$\mathbf{G}=<\mathbf{a}>=(\mathbf{Z_p},+)$

8.A_4是否是单群

答：

非也!

$1<K_4=\{(1),(12)(34),(13)(24),(14)(23)\}\lhd A_4$

9.$|G|=2n$，n为奇数，则$\exists H\lhd G, [G:H]=2$

证明：用Cayley定理，及其证明的方法

令$G'=\{f_a\mid a\in G, f_a(x)=ax\}$则$G\cong G'$

由于$f_a(a\ne e)$在G上无不动点，因而在f_a的对换分解式中每个元素均出现.

另一方面，由于$|G|=2n$，G中必有2阶元(习题2.5)，

设为b，则f_b可表为$f_b=(i_1j_1)(i_2j_2)\ldots\ldots(i_nj_n)$

由于n为奇数，f_b为奇置换，令

$H=\{f_a\mid f_a\text{是偶置换}\}$

则$[G:H]=2, \therefore H\lhd G$

习题 2.7

1.$G=GL_2(C), N=\{\begin{pmatrix}a&b\\0&d\end{pmatrix}\mid ad\ne 0\}, H=\{\begin{pmatrix}1&t\\0&1\end{pmatrix}\mid t\in C\}$

求$C(G), C_G(N), C_N(H), N_G(H)$

解：

(1)$C(G)=\{aI\mid a\in C^*\}$

(2)设$\begin{pmatrix}u&v\\w&x\end{pmatrix}\in G$

由$\forall\begin{pmatrix}a&b\\0&d\end{pmatrix}\in N$满足$\begin{pmatrix}u&v\\w&x\end{pmatrix}\begin{pmatrix}a&b\\0&d\end{pmatrix}=\begin{pmatrix}a&b\\0&d\end{pmatrix}\begin{pmatrix}u&v\\w&x\end{pmatrix}$

可得$v=w=0, u=x\ne 0$

$\therefore C_G(N)=C(G)$

(3)由$\begin{pmatrix}a&b\\0&d\end{pmatrix}\begin{pmatrix}1&t\\0&1\end{pmatrix}=\begin{pmatrix}1&t\\0&1\end{pmatrix}\begin{pmatrix}a&b\\0&d\end{pmatrix}$可得$a=d$

$\therefore C_N(H)=\{\begin{pmatrix}a&b\\0&a\end{pmatrix}\mid a\in C^*, b\in C\}$

(4)$N_G(H)=\{A\mid A\in G, AHA^{-1}=H\}$

由$\begin{pmatrix}a&b\\c&d\end{pmatrix}\begin{pmatrix}1&t\\0&1\end{pmatrix}(\frac{1}{ad-bc}\begin{pmatrix}d&-b\\-c&a\end{pmatrix})$

$=\frac{1}{ad-bc}\begin{pmatrix}ad-bc-act&a^2t\\-c^2t&ad-bc+act\end{pmatrix}\in H$

得$c=0$

$\therefore N_G(H)=\{\begin{pmatrix}a&b\\0&d\end{pmatrix}\mid a,b,d\in C, ad\ne 0\}=N$

2.$H\le G$证明

(1)$C_G(H)\lhd N_G(H)$

(2)$C_GC_GC_G(H)=C_G(H)$

证明：(1)

$C_G(H)=\{a\mid\forall h\in H,ha=ah\}=\{a\mid a\in G,\forall h\in H,aha^{-1}=h\}$

$N_G(H)=\{a\mid a\in G,aHa^{-1}=H\}$

由以上表达式可见$C_G(H)\le N_G(H)$

$\forall b\in N_G(H),a\in C_G(H)$,

由于$(bab^{-1})h(bab^{-1})^{-1}=ba(b^{-1}hb)a^{-1}b^{-1}=bah_1a^{-1}b^{-1}=bh_1b^{-1}=h$

$\therefore bab^{-1}\in C_G(H),C_G(H)\lhd N_G(H)$

(2)首先可证$H\le C_GC_G(H)$..........(*)

由于$\forall h\in H,a\in C_G(H)$有$ha=ah$,

$\therefore h\in C_GC_G(H),H\le C_GC_G(H)$

用$C_G(H)$代替(*)的中的H得$C_G(H)\le C_GC_GC_G(H)$

另一方面,当$A\le B$时,由中心化子的定义,

易见$C_G(A)\ge C_G(B)$,得出关系应用于(*)

得$C_G(H)\ge C_GC_GC_G(H)$

故$C_G(H)=C_GC_GC_G(H)$

3.$|G|<\infty,H<G$,G中与H共轭的全部子群为$H_1,H_2,\dots\dots,H_k$则$\bigcup_{i=1}^{k}H_i<G$

证明：

当$k=1$时,显然成立

下设$k\ge 2$,由于$k=[G:N_G(H)]\le[G:H]$

考虑到$e\in H_i\ (i=1,2,\dots\dots,k)$

因而$|\bigcup_{i=1}^{k}H_i|\le k|H|-(k-1)<k|H|<[G:H]\cdot|H|=|G|$

故$\bigcup_{i=1}^{k}H_i<G$

4.$|G|=p^2$(p为素数)$\Rightarrow G$可换

证明：（利用非平凡中心定理）

由2。7例3知G中有非平凡中心C,

且$|C|\,|\,p^2$

若$|C|=p$，则有$a\in G\setminus C$且$G>C_G(a)>C$

因而$p\,|\,|C_G(a)|,|C_G(a)|\,|\,p^2$

故$|C_G(a)|=p^2$，$a\in C$,矛盾

因而$|C|=p^2$,

$\therefore G$是可换群

5.$|G|=pq$(p,q为互异素数)，且$p<q$，则G中的q阶子群是正规子群。

证明：设H为q阶子群，若H不是正规子群，

则存在$a\in G$使$aHa^{-1}\ne H$，因而可得

$|H(aHa^{-1})|=q^2>|G|$

与$H(aHa^{-1})\subseteq G$矛盾

$\therefore H$为正规子群。

6.$|G|=p^n$(p为素数)$\Rightarrow G$中非正规子群的个数是p的倍数.

证明：（利用共轭子群类及定理）

设H为任一非正规子群，$K_H=\{gHg^{-1}\mid g\in G\}$

由于$H\le N_G(H)<G,|N_G(H)|=p^r,r<n$

因而$|K_H|=[G:N_G(H)]>1$

由$Lagrange$定理知$|K_H|=p^\alpha,1\le\alpha<n$

故全部非正规子群的个数为$m=\sum_{\substack{H\le G\\ H\text{非正规}}}|K_H|$

$\therefore p\mid m$

7.证明S_n中$1^{\lambda_1}2^{\lambda_2}\dots\dots n^{\lambda_n}$型置换的个数为$\dfrac{n!}{1^{\lambda_1}2^{\lambda_2}\dots\dots n^{\lambda_n}\cdot\lambda_1!\lambda_2!\dots\lambda_n!}$

证明：设σ为$1^{\lambda_1}2^{\lambda_2}\dots n^{\lambda_n}$型置换，则可表为

$\sigma=\underbrace{(*)\dots(*)}_{\lambda_1\text{个}}\underbrace{(**)\dots(**)}_{\lambda_2\text{个}}\dots\dots\underbrace{(**\dots**)}_{\lambda_n\text{个}}$

任何一个n元排列是一个该类的置换，但与同一个轮换中起始元素的选择无关，因而应除以因子k^{λ_k}；在相同长度的轮换中，与排列的次序无关，故应除以因子$\lambda_k!$。

8.确定A_4中的共轭类与正规子群。

解：按类型分析如下：$K_1=\{(1)\}$

在1^13^1－型中，由于$C_{S_4}(\sigma)=\{(1)\}$，故可分为两类：

$K_2=\{(123),(142),(134),(243)\}$

$K_3=\{(132),(124),(143),(234)\}$

2^2－型只有一类：

$K_4=\{(12)(34),(13)(24),(14)(23)\}$

9.确定二面体群D_6的共轭类与正规子群.

解：

(1) $K_{(1)}=\{(1)\}$

(2) 对$\{\pi_i\}$：由于$\rho_k\pi_l\rho_k^{-1}=\pi_{2k+l},\pi_k\pi_l\pi_k^{-1}=\pi_{2k-l}$

故得两类：

$K_{\pi_0}=\{\pi_0,\pi_2,\pi_4\},K_{\pi_1}=\{\pi_1,\pi_3,\pi_5\}$

(3)对$\{\rho_i\}$：$\rho_2=(135)(246)$,由$\pi_0\rho_2\pi_0^{-1}=\rho_4$

$\therefore K_{\rho_2}=\{\rho_2,\rho_4\}\quad K_{\rho_3}=\{\rho_3\}$

$K_{\rho_1}=\{\rho_1,\rho_5\}(\because\pi_0\rho_1\pi_0^{-1}=\rho_5)$

正规子群：

$\{(1)\},D_6,<\rho_1>,\{\rho_0\}\cup K_{\rho_2}\cup K_{\pi_0},\{\rho_0\}\cup K_{\rho_2}\cup K_{\pi_1}$

10.$G=\left\{\begin{pmatrix}1&0\\a&\varepsilon\end{pmatrix}\mid\varepsilon=\pm1,a\in Z\right\}$确定全部共轭类和正规子群。

解：取定n，可得

(1)$\overline{\begin{pmatrix}1&0\\n&1\end{pmatrix}}=\left\{\begin{pmatrix}1&0\\a&\varepsilon\end{pmatrix}\begin{pmatrix}1&0\\n&1\end{pmatrix}\begin{pmatrix}1&0\\a&\varepsilon\end{pmatrix}^{-1}\mid\varepsilon=\pm1,a\in Z\right\}$

$=\left\{\begin{pmatrix}1&0\\n&1\end{pmatrix},\begin{pmatrix}1&0\\-n&1\end{pmatrix}\right\}$

$n=0,1,2,\dots\dots$

$\overline{\begin{pmatrix}1&0\\n&-1\end{pmatrix}}=\left\{\begin{pmatrix}1&0\\a&\varepsilon\end{pmatrix}\begin{pmatrix}1&0\\n&-1\end{pmatrix}\begin{pmatrix}1&0\\a&\varepsilon\end{pmatrix}^{-1}\mid\varepsilon=\pm1,a\in Z\right\}$

$=\left\{\begin{pmatrix}1&0\\2a+\varepsilon n&-1\end{pmatrix}\mid\varepsilon=\pm1,a\in Z\right\}$

(2)当$n=2m$时，得$\overline{\begin{pmatrix}1&0\\0&-1\end{pmatrix}}=\left\{\begin{pmatrix}1&0\\2m&-1\end{pmatrix}\mid m\in Z\right\}$

(3)当$n=2m+1$时，得

$\overline{\begin{pmatrix}1&0\\0&-1\end{pmatrix}}=\left\{\begin{pmatrix}1&0\\2m+1&-1\end{pmatrix}\mid m\in Z\right\}$

由共轭类型成的以下三类共轭子群：

由第（1）类共轭类形成的正规子群为：

$H_k=\left\{\begin{pmatrix}1&0\\nk&1\end{pmatrix}\mid n\in Z\right\},k=0,1,2,\dots\dots$

由H_2与第（2）类共轭类形成的正规子群为

$N_1=\overline{\begin{pmatrix}1&0\\1&-1\end{pmatrix}}\cup H_2$

由H_2与第（3）类形成

$N_2=\overline{\begin{pmatrix}1&0\\1&-1\end{pmatrix}}\cup H_2$

其余不可能形成正规子群。

习题 2.8

1.设$f:G\to G_1$同态，$\varphi:G_1\to G_2$同态,则$\varphi\circ f$是$G\to G_2$的同态

证明：$\forall a,b\in G,\varphi\circ f(ab)=\varphi(f(a)f(b))=\varphi(f(a))\cdot\varphi(f(b))$
$\therefore\varphi\circ f$是G到G_2的同态

2.$G=\{(a,b)\mid a,b\in R,a\neq 0\},(a,b)(c,d)=(ac,ad+b)$
$K=\{(1,b)\mid b\in R\}$
证明：$G/K=(R^*,\bullet)$

证明：作映射$f:(a,b)\to a(G\to R^*)$
$f((a,b)(c,d))=f(ac,ad+b))=ac=f(a,b)\bullet f(c,d)$
又f显然是满射
$\ker(f)=\{(a,b)\mid f(a,b)=1\}=\{(1,b)\mid b\in R\}=K$
$\therefore$由同态基本定理得$G/K\cong R^*$

3.G为有限$Abel$群，证明$f:g\mapsto g^k$是自同构的充分必要条件为$(k,|G|)=1$

证明:
$\Rightarrow$：反证法。假设$(k,|G|)\neq 1$，则有素数$p\mid k$和$p\mid |G|$，由有限$Abel$群性质:2.6例5
G中有p阶元a，即$a^p=e$，$a^k=e$故$\ker f=\{a\mid a^k=e\}\neq\{e\}$
与f是自同构矛盾。
$\Leftarrow$：首先f是同态：$f(g_1g_2)=(g_1g_2)^k=g_1^kg_2^k=f(g_1)f(g_2)$
再证$\ker f=\{e\}$，反证法。假设$\ker f\neq\{e\}$
则有$g\neq e$，使$g^k=e$，因而$o(g)\mid k,o(g)\mid |G|$
与$(k,|G|)=1$矛盾。

4.$G=(Z,+),G'=<a>$ 6阶循环群，$\varphi:n\to a^n$则φ是G到G'的同态
(1) 找出象为$<a^2>$的G的所有子群
(2) 找出中其象为$<a^3>$的所有子群。

证明：可设$G'=(Z_6,+),\varphi:n\mapsto\overline{n}$
$\varphi(n_1+n_2)=\overline{n_1+n_2}=\overline{n_1}+\overline{n_2}=\varphi(n_1)+\varphi(n_2)$
$\therefore\varphi$是G到G'的同态。
(1) 设$H_m=<m>\leq G,\varphi(H_m)=<\overline{2}>$
则$\varphi(m)=\overline{2}$或$\varphi(m)=\overline{4}$
即$\overline{m}=\overline{2}$或$\overline{m}=\overline{4}$
$\therefore m=6k+2$或$m=6k+4$
故全部子群为:$<6k+2>,<6k+4>,k=0,1,2,......$
(2) 设$H_m=<m>\leq G,\varphi(H_m)=<\overline{3}>$
则$\varphi(m)=\overline{3}$即$\overline{m}=\overline{3}$
$\therefore m=6k+3$,因而全部子群为:$<6k+3>,k=0,1,2,......$
分析：$G=(Z,+),G'=Z_6,\varphi:n\mapsto\overline{n},H'=<\overline{2}>$
$\varphi^{-1}(H')=<2>\because H'=<\overline{2}>=<\overline{4}>$,取$a,b,\varphi(a)=2,\varphi(b)=4$
则$\varphi(<a>)=H',\varphi(<b>)=H',a=6m+2,b=6m+4$

5.用同态基本定理证明$Q/Z\cong U=\{a\mid a\in C,a^n=1,n\in Z^+\}$

证明：U可表为$U=\{e^{\frac{i2k\pi}{n}}\mid n\in Z^+,k=0,1,\ldots,n-1\}$
作映射$f:q\mapsto e^{iq2\pi}$
$f(q_1+q_2)=e^{i(q_1+q_2)2\pi}=e^{iq_12\pi}e^{iq_22\pi}=f(q_1)f(q_2)$
显然是满射。$\ker f=\{q\mid e^{iq2\pi}=1\}=Z$
$\therefore Q/Z\cong U$

6.求$(Z,+)$上的所有自同态.

并证明它与 Z 的乘法半群同构。
解：设f是$(Z,+)$上的任一自同态，可令
$f(1)=m$,则$f(k)=km$，令$f_m:k\mapsto km$
则$End(Z,+)=\{f_m\mid f_m(k)=km,m=0,1,2,\ldots\ldots\}$

设$\wp$: $f_m\mapsto m(End(Z,+)\to(Z,\cdot))$,
因为$f_{mn}(x)=mnx=f_m(f_n(x))$,
故$f_{mn}=f_m\cdot f_n$,
得$\wp(f_mf_n)=\wp(f_{mn})=mn=\wp(f_m)\wp(f_n)$,
又$\wp$显然是双射.
所以$End(Z,+)$与$(Z,\cdot)$同构.

7.求$(Z_n,+)$上的全部自同态与自同构.

解:
(1)设f是Z_n上任意一个自同态，可设$f(\overline{1})=\overline{m}$
则$f(\overline{k})=\overline{km}$，令$f_m:\overline{k}\mapsto\overline{km}$
$\therefore End(Z_n,+)=\{f_m\mid f_m(\overline{k})=\overline{km},m=0,1,2,\ldots,n-1\}$
(2) $f_m\in Aut(Z_n,+)\Leftrightarrow f_m$是双射
$\Leftrightarrow\exists\overline{k}$使$f_m(\overline{k})=\overline{1}\Leftrightarrow\overline{km}=\overline{1}\Leftrightarrow(m,n)=1$
$\therefore Aut(Z_n,+)=\{f_m\mid f_m(\overline{k})=\overline{mk},(m,n)=1,1\leq m<n\}\cong(Z_n^*,\bullet)$

8.设K_4为$Klein$四元群，求$AutK_4$。

解：$K_4=\{e,a,b,c\}$令$f=\begin{pmatrix}e&a&b&c\\e&x_1&x_2&x_3\end{pmatrix}$
x_1,x_2,x_3为a,b,c的一个排列
$f(ab)=f(c)=x_3=x_1x_2=f(a)f(b)\therefore f\in AutK_4$
故$AutK_4\cong S_3$

9.$G=GL_n(R)$,求$InnG$

解：$InnG=\{\varphi_A\mid\varphi_A(X)=AXA^{-1},A\in G\}$
由于$C(G)=\{aI\mid a\in R^*\}$
$G/C(G)=\{\overline{A}\mid A\in G,|A|=1\}$
由定理6$\therefore InnG\cong G/C(G)=\{\overline{A}\mid A\in G,|A|=1\}$

10.设G是单群，且可不交换，则$G\cong InnG$

证明:$\because C(G)\lhd G$,且不可换,$\therefore C(G)=\{e\}$
故$InnG\cong G/C(G)=G$

11.设G有有限个子群，f是G的满自同态，证明：f是G的自同构。

证明：只需证明$\ker f=\{e\}$
设$K=\ker f$,
$S=\{H\mid K\le H\le G\},T=\{H\mid H\le G\}$
显然$S\subseteq T$，若$K\ne\{e\}$，则$\{e\}\notin S,\{e\}\in T$
故$|S|\ne|T|$，f不可能是S到T的双射，
与子群对应定理矛盾。

第 2 章 习题 2.9 第 1 题解答

1.设G作用于X上，$a\in X$,证明$b\in\Omega_a\Leftrightarrow\Omega_a=\Omega_b$

证明：
$\Omega_a=\{g(a)\mid g\in G\},b\in\Omega_a\Rightarrow\exists g_1\in G:g_1(a)=b,a=g_1^{-1}(b)$
$\forall g(a)\in\Omega_a,g(a)=gg_1^{-1}(b)\in\Omega_b,\therefore\Omega_a\subseteq\Omega_b$
类似可证$\Omega_b\subseteq\Omega_a$
反之，显然。

2.证明：$G_{g(a)}=gG_ag^{-1}$

$\forall\sigma\in G_{g(a)},\sigma(g(a))=g(a),g^{-1}\sigma g(a)=a$
$g^{-1}\sigma g\in G_a,\therefore\sigma\in gG_ag^{-1},G_{g(a)}\subseteq gG_ag^{-1}$
反之,$\forall g\tau g^{-1}\in gG_ag^{-1},g\tau g^{-1}(g(a))=g(a)$
$\therefore g\tau g^{-1}\in G_{g(a)},G_{g(a)}\supseteq gG_ag^{-1}$
综上$G_{g(a)}=gG_ag^{-1}$

3.$H\le G,\Omega=\{aH\mid a\in G\}$,$G$对$\Omega$的作用为
$g(aH)=gaH$
证明满足群对集合作用之定义，并求Ω_{aH}与G_{aH}

证明:
(1)$e(aH)=aH$
(2)$g_1g_2(aH)=g_1g_2(aH)=g_1(g_2(aH))$
$\Omega_{aH}=\{g(aH)\mid g\in G\}=\Omega$
$G_{aH}=\{g\mid g(aH)=aH\}=\{g\mid a^{-1}ga\in H\}=\{g\mid g\in aHa^{-1}\}=aHa^{-1}$

4.$|G|<\infty,\Omega=\{K\mid K\subseteq\Omega,|K|=k\}$,$G$对$\Omega$的作用为：$g(K)=gK$
证明满足定义，问是否可迁？

证明：
(1)$e(K)=K$,(2)$g_1g_2(K)=g_1(g_2(K))$,$\Omega_K=\{gK\mid g\in G\}$,
当$k=1$时，可迁
当$2\le k\le n-2$时，设$|G|=n,|\Omega|=\binom{n}{k}$,则$|G|<|\Omega|$
若可迁,则$|G|=|G_a||\Omega_a|=|G_a||\Omega|,|G|\ge|\Omega|$，矛盾.
故不可迁。
当$k=n-1$时，可证是可迁的：
设$a\notin K_1$，$b\notin K_2$
取g_1满足$g_1=ba^{-1}$，而$a=g_1^{-1}b$,则$b\notin g_1K_1$
否则$\exists c:b=g_1c,c=g_1^{-1}b=a\in K_1$矛盾
因而$g_1K_1=K_2$

5.G对Ω的作用$\sigma_g:x\mapsto g(x)$
证明：
(1)σ_g是Ω上的一个置换。
(2)$\varphi:g\mapsto\sigma_g$是G到S_Ω上的同态。

证明:
(1)只需证σ_g是Ω上的单射:
$\sigma_g(x_1)=\sigma_g(x_2)\Rightarrow g(x_1)=g(x_2)\Rightarrow g^{-1}g(x_1)=x_2\Rightarrow e(x_1)=x_1=x_2$
(2)$\varphi(g_1g_2)(x)=\sigma_{g_1g_2}(x)=g_1g_2(x)=g_1(g_2(x))=\sigma_{g_1}\sigma_{g_2}(x)=\varphi(g_1)\varphi(g_2)(x)$
保持运算

第 2 章 习题 2.10 第 1 题解答

1.用 3 种颜色做成 5 颗珠子的项链，可做成多少种？

$D_5,\Omega=\{f\mid f:\{1,2,3,4,5\}\mapsto\{a_1,a_2,a_3\}\},|\Omega|=3^5$

g 的类型	X(g)	同类 g 的个数	∑X(g)
1^5	3^5	1	3^5
5^1	3	4	4*3
1^12^2	3^3	5	$5*3^3$
∑		10	

$N=\frac{1}{10}\times3(3^4+4+5\times3^2)=\frac{3}{10}(81+4+45)=39$
∴共有39种。

2. 在苯环上结合 3 个 H 和 3 个 CH3,可形成多少种化合物？
解 熟悉 Burnside 定理，并掌握应用方法。
方法要点：搞清置换群和目标集；作表计算不动点数。
置换群为 D6,目标集Ω为有标号的正 6 边形的顶点着色，|Ω|=C63=20。作下表：

g(G 中元素)的类型	χ(g)—g 在Ω中的不动点数	同类 g 的个数	Σ χ(g)
16	20	1	20
1222	4	3	12
23	0	4	0
32	2	2	4
61	0	2	0
Σ		12	36

所以 N=36/12=3。
共可形成 3 种化合物。
3. 对正 6 面体的面用 n 种颜色着色，问有多少种本质上不同的着色方法？
解 熟悉 Burnside 定理，并掌握应用方法。

方法要点：搞清置换群和目标集；作表计算不动点数。

置换群为 S4,目标集Ω为正 6 面体的有标号的面着色，|Ω|=n6。

作下表：

g(G 中元素)的类型	χ(g)—g 在Ω中的不动点数	同类 g 的个数	Σχ(g)
16	n6	1	n6
1241	n3	6	6 n3
23	n3	6	6 n3
32	n2	8	8 n2
1222	n4	3	3n4
Σ		24	n6+3n4+12 n3+8n2

所以本质上不同的着色方法数为

N=(n6+3n4+12 n3+8n2)/24。

4. 求 5 个点的不同构的图有多少个？

解 熟悉 Burnside 定理，并掌握应用方法。

方法要点：搞清置换群和目标集；作表计算不动点数。

置换群为 S5，目标集Ω为 5 个点的有标号图的集合，|Ω|=210。

作下表：

g(G 中元素)的类型	χ(g)—g 在Ω中的不动点数	同类 g 的个数	Σχ(g)
15	210	1	210
1321	27	10	10×27
1231	24	20	20 ×n3
1141	23	30	30×23
1122	26	15	15×26
2131	23	20	20×23
51	22	24	24×22
Σ		120	4080

所以 5 个点的不同构的图的个数为

N=4080/120=34。

2.11

1. 设 G 是群，G_1, G_2是 G 的正规子群，且 G=< G_1, G_2>, $G_1∩G_2$={e}, 证明

$G≌G_1×G_2$ 。

证 由本节定理 2，只需证明 $G= G_1G_2$ 。

显然有 G_1G_2 属于 G。

反之，任取 g∈G, 因 g∈< G_1, G_2> 和 G_1, G_2 是 G 的正规子群，g 可表为

g=ab, a∈G_1，b∈G_2 ，

所以 g∈G_1G_2 。

综上和由本节定理 2，得 $G= G_1G_2≌G_1×G_2$ 。

2．证明 Z/(6)≌Z/(2)×Z/(3)。

证 首先要理解符号的意义。实际上就是证明以下命题：

$(Z_6, +)≌(Z_2, +)×(Z_3, +)$ 。

利用本节定理 2，要证三条。但与定理 2 的条件还有些问题，$(Z_2, +)$ 与 $(Z_3, +)$ 还不能直接看作是$(Z_6, +)$的子群，为此，令

G=（Z_6, +)={0，1，2，3，4，5}，其中 k 表示 k 模 6 的同余类。

G_1={0，3}， G_2={0，2，4}，

则 $G_1≌(Z_2, +)$，$G_2≌(Z_3, +)$ 。

由于（1）G_1，G_2 是 G 的正规子群，

（2）G= G_1+ G_2，

（3）$G_1∩G_2$={0}。

所以 $(Z_6, +)≌G_1+G_2≌(Z_2, +)×(Z_3, +)$ 。

3. 设 $G=G_1×G_2$，证明 $G/G_1≌G_2$, $G/G_2≌G_1$ 。

证 首先看清题目，发现 G_1，G_2 并不是 G 的子群，因此必是同构的关系。

令 H= G_1×{e}，则 H≤G, 且 H≌G_1; N={e}×G_2，则 N≤G, 且 N≌G_2 。

这样商群 G/G_1 与 G/G_2 有意义。

接着要证 H 和 N 是 G 的正规子群：

任取 (a,b)∈G, (c,e)∈H，有

$(a,b)(c,e)(a,b)^{-1}=(aca^{-1},e)$ ∈H,

所以 H 是 G 的正规子群。

作映射 f: (a,b)→b (G→G_2),

由于 $f((a_1,b_1)(a_2,b_2))=f((a_1a_2,b_1b_2))=b_1b_2$

$=f(a_1,b_1)f(a_2,b_2)$,

所以 f 是同态映射，且显然是满射，f 是满同态映射。

求核：

ker f={(a,b)|f(a,b)=b=e}={(a,e)|a∈G_1}

= G_1×{e}=H≌G_1。

由同态基本定理，得

$G/G_1≌G_2$ 。

类似可证 $G/G_2≌G_1$ 。

4. 纱 A, B≤G, G=A×B, N≤A 且是正规子群。证明

G/N≌(A/N)×B 。

证 首先看一下题的意义。N 是 A 的子群，不直接是 G 的子群，但 N×{e}是 G 的子群，而 N×{e}≌N，因而 G/N≌G/ N×{e}。

设 A/N={aN|a∈A},

作映射 f: (a,b)→(aN,b) (G→(A/N)×B),

由于 $f((a_1,b_1)(a_2,b_2))=f(a_1a_2,b_1b_2)=(a_1a_2N,b_1b_2)$

$=(a_1N,b_1)(a_2N,b_2)=f(a_1,b_1)f(a_2,b_2)$,

所以 f 是同态，且显然是满同态。

求核：

ker(f)={(a,b)|f(a,b)=(N,e)}= {(a,b)|(aN,b)=(N,e)}

={(a,b)|a∈N,b=e)}=(N,e)= N×{e}≌N 。

故由同态基本定理得

G/N≌(A/N)×B 。

5. 写出 45 阶可换群的一切可能的类型。

解 由于 $45=5\times3^2$, 45 的初等因子组有：

$\{5, 3^2\}$, {5, 3, 3}。

不变因子组有：

{45}, {15, 3}。

所以 45 阶可换群的一切可能的类型有：

C_{45}，$C_{15}\times C_3$ 。

6. 写出 144 阶可换群的一切可能的类型。

解 由于 $144=2^4\times3^2$, 144 的初等因子组有：

$\{2^4, 3^2\}$, $\{2^3, 2, 3^2\}$, $\{2^2, 2^2, 3^2\}$, $\{2^2, 2, 2, 3^2\}$, $\{2, 2, 2, 2, 3^2\}$, $\{2^4, 3, 3\}$, $\{2^3, 2, 3, 3\}$, $\{2^2, 2^2, 3, 3\}$, $\{2^2, 2, 2, 3, 3\}$, {2, 2, 2, 2, 3, 3}。

不变因子组有：

{144}, {72, 2}, {36,4}, {36,2,2}, {18, 2,2,2},

{48, 3}, {27,6}, {12,12}, {12, 6,2}, {6,6,2,2}。

所以 144 阶可换群的一切可能的类型有：

C_{144}，$C_{72}\times C_2$，$C_{36}\times C_4$，$C_{36}\times C_2\times C_2$，$C_{18}\times C_2\times C_2\times C_2$，

$C_{48}\times C_3$，$C_{27}\times C_6$，$C_{12}\times C_{12}$，$C_{12}\times C_6\times C_2$，$C_6\times C_6\times C_2\times C_2$ 。

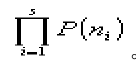
7. 试求 n 阶交换群的可能的类型数。

解 设 n 的素因子分解式为

$n=p_1^{n1}p_2^{n2}...p_s^{ns}$ 。

设 P(m) 为整数 m 的分拆数，例如，4 可分拆为：4, 3+1, 2+2, 2+1+1, 1+1+1+1。所以 P(4)=5，一般的公式见组合数学的书。

由此得 n 阶交换群的可能的类型数为


$\prod_{i=1}^{s} P(n_i)$ 。

第 2 章 习题 2.12 第 1 题解答

证明：145 阶群是循环群.

证：

$|G| = 145 = 5\times29$,

显然,29阶Sylow子群的个数为1,设为P_{29},则$P_{29} \lhd G$.

5阶Sylow子群的个数为$N(5^1) = 5q+1$,由$N(5^1)|145$,得$N(5^1) = 1$.

因而有$P_5 \lhd G$.

所以$G = C_5 \times C_{29} = C_{145}$.

2.确定S_4的不同的Sylow子群的个数.

解:$|S_4| = 24 = 2^3\times3$

(1).$N(3) = 3k+1, N(3)|24, \therefore k = 0$或1.由于$S_4$中有不只一个3阶元,$\therefore N(3) = 4$.

(2).$N(2^3) = 2k+1, N(2^3)|24, \therefore k = 0$或1,当$N(2^3) = 1$时,Sylow2 - 群$P \lhd G$.

这时P中必有4阶元δ,由于$K_\delta = \{g\delta g^{-1} | g\in G\}\subseteq P$,即所有$4^1$ - 型置换和2^2 - 型置换均在P中,$|P|>8$,矛盾.故$N(2^3) = 3$.

$\therefore S_4$中有3个8 - 群和4个3 - 群.

4个3 - 群为:<(123)>,<(124)>,<(134)>,<(234)>.

3个8 - 群为:<(1234),(24)>,<(1324),(34)>,<(1243),(23)>.

3.证明40阶群不是单群.

证:$|G| = 40 = 2^3\times5, N(2^3) = 2k+1, N(2^4)|40. \therefore k = 0$或2.

$N(5) = 5l+1, N(5)|40. \therefore l = 0. \therefore N(5) = 1$.

故5 - 子群是正规子群.

4.p,q是素数,证明pq阶群不是单群.

证:分两种情形讨论:

(1).p = q, $|G| = p^2$, G有非平凡中心,且C中有p阶元α, $<\alpha>\lhd G$,

$\therefore G$非单群.

(2).$p\neq q$,可设$p>q$,由存在定理,存在p - 群P,若有$g\in G$,使$gPg^{-1}\neq P$,

则$|P(gPg^{-1})| = P^2>|G|$,矛盾.$\therefore \forall g\in G$,均有$gPg^{-1} = P$, $P\lhd G$, G非单群.

方法二:(2)$p\neq q$,可设$p>q$, $N(p) = kp+1$及$N(p)|pq$,当$k\geq1$时,$N(p)$不整除$pq. \therefore k = 0, N(p) = 1$, G中有唯一p - 群P, $P\lhd G, \therefore G$不是单群.

5.$p\,|\,|G|, N\lhd G, (p,|G/N|) = 1 \Rightarrow N$ 包含所有的Sylow p - 子群.

证:设$|G| = p^\alpha n_1, (p,n_1) = 1$,

$|N| = p^\beta n_2, (p,n_2) = 1$.

由于p不整除$|G/N|$,得$\alpha = \beta$,

$|N| = p^\alpha n_2, (p,n_2) = 1$.

因而N也包含Sylow p - 子群P,又由

于$N\lhd G, \forall g\in G, gPg^{-1}\subseteq N$.

即N包含所有Sylow p - 子群.

第 3 章 习题 3.1 第 1 题解答

1.$(A,+,\cdot)$是环，A^A中定义$(f\oplus g)(x) = f(x)+g(x)$，$f\cdot g(x) = f(x)g(x)$，证明$(A^A,\oplus,\cdot)$是环。若定义$(f\oplus g)(x) = f(x)+g(x)$，$f\cdot g(x) = f(g(x))$，$(A^A,\oplus,\cdot)$是否是环？

证明：主要验证分配律：

$f\cdot(g\oplus h)(x) = f(x)\cdot(g\oplus h)(x) = f(x)g(x)+f(x)h(x) = (f\cdot g\oplus f\cdot h)(x)$

类似可证右分配律。

但对第二种定义，分配律不成立：

$f\cdot(g\oplus h)(x) = f(g(x)+h(x))$

$(f\cdot g\oplus f\cdot h)(x) = f(g(x))+f(h(x))$

两者不一定相等，故$(A^A,\oplus,\cdot)$不一定是环。

例如：在$(R,+,\cdot)$上$f(x) = x^2, g(x) = x, h(x) = 2x$.左分配律不成立

2.求Klein四元群的自同态环的所有元素。

解:

$\because K_4 = \{e,a,b,c\} = <a,b\,|\,o(a) = o(b) = 2, ab = ba>$

$\forall f\in E(K_4), f(e) = e, f(c) = f(a)f(b)$

故f由f(a)与f(b)所决定，因此全体$E(k_4)$的元素为

$$E(K4) = \left\{ f_{xy} = \begin{pmatrix} e & a & b & c \\ e & x & y & xy \end{pmatrix} \,|\, x,y\in K_4 \right\}$$

且$|E(K_4)| = 16$

3.证明：$M_N(Z)$中每一左零因子也是右零因子。

证明：设$AB=0$，$A\neq 0, B\neq 0$，则秩$(A)=r<n$

不妨设A的前r个行向量线性无关，其余向量可用它们线性表出，因而可左乘一可逆阵$C\in M_n(Z)$

使$CA=\begin{bmatrix}\alpha_1\\ \vdots\\ \alpha_2\\ 0\\ \vdots\\ 0\end{bmatrix}$，取$D=\begin{bmatrix}0&\vdots&0&1&\vdots&1\\0&\vdots&0&1&\vdots&1\\ \vdots&\vdots&\vdots&\vdots&\vdots&\vdots\\0&\vdots&0&1&\vdots&1\end{bmatrix}$（$r$列零，$n-r$列1），则$DCA=0$

显然$DC\neq 0$，$DC\in M_n(Z)$，$\therefore A$是右零因子。

4.整环中除零元外无其它的幂零元，除零元与单位元外无其它的幂等元。

证明：

(1) 设$a^n=0$，且$a\neq 0$，则由消去律可得$a=0$，矛盾。

(2) 设$a^2=a$，且$a\neq 0$，可证a必为单位元：

$\forall x\in A$有$a^2x=ax$，由消去律得$ax=x$，

$\therefore a$是左单位元，类似可证a也是右单位元，故a是单位元。

5.$\Gamma=\{f(x)\mid [0,1]$上的实连续函数$\}$

定义$+:(f+g)(x)=f(x)+g(x)$;

$\cdot:(f\cdot g)(x)=f(x)g(x)$

证明：

(1)$(\Gamma,+,\cdot)$是环

(2) f是零因子 $\Leftrightarrow$ f的零点包含一个开区间

(3) 并求Γ中的幂零元，幂等元，逆元

证与解：

(1) 由连续函数性质可得，$(\Gamma+)$是加群，$(\Gamma,\cdot)$是半群。易验证满足分配律。

(2) 设$fg=0$，$f\neq 0, g\neq 0$，则$\exists x_0\in[0,1]$，使$g(x_0)\neq 0$

$\Rightarrow$:由连续函数的性质，$\exists\varepsilon$使$g(x)$在$(x_0-\varepsilon,x_0+\varepsilon)$上不为零，因而$f(x)$在$(x_0-\varepsilon,x_0+\varepsilon)$上为0

$\Leftarrow$:设$f(x)$在区间(a,b)上为零，则f的非零集非空，即$f(x)\neq 0$，于是可取$g(x)$为

$g(x)\neq 0$在(a,b)上；$g(x)=0, x\notin(a,b)$，这样的连续函数很容易做出。因$fg=0$，f是零因子。

(3) Γ中的幂零元：设$[f(x)]^n=0$，可得$f(x)=0,\forall x\in[0,1]$

Γ中的幂等元：$[f(x)]^2=f(x)$，可得$f(x)(f(x)-1)=0$

$\forall x\in[0,1]$，有$f(x)=0$或$f(x)=1$，又连续函数的性质得$f(x)=0,\forall x\in[0,1]$或$f(x)=1,\forall x\in[0,1]$

Γ中的逆元：$f(x)g(x)=1\Leftrightarrow\forall x\in[0,1], f(x)\neq 0$，即$f(x)$在$[0,1]$上无零点

6.确定$M_n(Z)$中的幂零元

解：设$A\in M_n(Z), A^n=0$

考虑A在复数域上的约当标准形：

$$P^{-1}AP=\begin{bmatrix}\lambda_1&*&*\\0&\ddots&*\\0&0&\lambda_n\end{bmatrix}=\Lambda$$

则$A^n=P\Lambda^nP^{-1}=0$

反之，若有$\lambda_i\neq 0$，则$A^k\neq 0,\forall k\in Z^+$

$\therefore$ 全体幂零元$=\{A\mid A\in M_n(Z), A$在C中的特征值全为$0\}$

7.证明环中的元素u可逆$\Leftrightarrow$

或(1)$uvu=u, vu^2v=1$成立或(2)$uvu=u$，且v是唯一满足此条件的元素。

证明：

$\Rightarrow$: 显然成立

$\Leftarrow$: (1) $uvu=u, vu^2v=1\Rightarrow vuvu^2v=vu^2v\Rightarrow vu=1$

类似可证$uv=1$

(2) 令$v_1=v+vux-x$,

$uv_1u=uvu+uvuxu-uxu=u$

由v的唯一性，得$v_1=v, vux=x$

$\therefore vu=1$，类似可证$uv=1$

$\therefore u$可逆

8.(华罗庚) $a,b,ab-1$可逆$\Rightarrow a-b^{-1},(a-b^{-1})^{-1}-a^{-1}$，可逆且$[(a-b^{-1})^{-1}-a^{-1}]^{-1}=aba-a$

证：

$ab-1=(a-b^{-1})b, \therefore (a-b^{-1})^{-1}=b(ab-1)^{-1}$

$(a-b^{-1})^{-1}-a^{-1}=(a-b^{-1})^{-1}(1-(a-b^{-1})a^{-1})=(a-b^{-1})^{-1}b^{-1}a^{-1}$

$\therefore[(a-b^{-1})-a^{-1}]^{-1}=ab(a-b^{-1})=aba-a$

9* 证明：$a,b\in A$，若$1-ab$可逆，则$1-ba$可逆

证明：

方法一：（用级数）

定义$(1-ab)^{-1}=1+ab+(ab)^2+\ldots\ldots$

则$(1-ab)^{-1}=1+a(1+ba+(ba)^2\ldots\ldots)b=1+a(1-ba)^{-1}b$

所以有$(1-ba)^{-1}=1+b(1-ab)^{-1}a$

方法二：

$$\begin{bmatrix}1&0\\-a&1\end{bmatrix}\begin{bmatrix}1&b\\a&1\end{bmatrix}=\begin{bmatrix}1&b\\0&1-ab\end{bmatrix},\begin{bmatrix}1&-b\\0&1\end{bmatrix}\begin{bmatrix}1&b\\a&1\end{bmatrix}=\begin{bmatrix}1-ba&0\\a&1\end{bmatrix}$$

$$\begin{bmatrix}1&b\\a&1\end{bmatrix}^{-1}=\begin{bmatrix}1&-b\\0&1\end{bmatrix}\begin{bmatrix}1&0\\0&(1-ab)^{-1}\end{bmatrix}\begin{bmatrix}1&0\\-a&1\end{bmatrix}$$

$$=\begin{bmatrix}1&0\\-a&1\end{bmatrix}\begin{bmatrix}(1-ba)^{-1}&0\\0&1\end{bmatrix}\begin{bmatrix}1&-b\\0&1\end{bmatrix}$$

比较左上角元素。

10.设u有右逆，证明以下命题等价：

(1) u有多于一个右逆

(2) u不是可逆元

(3) u是左零因子

证：

(1)$\Rightarrow$(2)：设u有两个右逆元v_1,v_2，则$uv_1=uv_2=1$

若u是可逆元，则得$v_1=v_2=u^{-1}$，矛盾

(2)$\Rightarrow$(3)：设$uv=1$，则$vu\neq 1$，因而$uvu=u, u(vu-1)=0$

$\because vu\neq 1, \therefore u$是左零因子

(3)$\Rightarrow$(1)：设$uw=0, uv=1$，则$v_1=v+w\neq v$，也是右逆。

11.(*Kaplansky*)如果环中一个元素有多于一个右逆，则有无穷多个右逆。

证明：

设$uv_1=1, uv_2=1$，且$v_1\neq v_2$

令$v_k=v_1+v_{k-1}u-1\,(k=3,4,..)$

则$uv_k=uv_1+uv_{k-1}u-u=1, k=3,4,\ldots.$

$\therefore v_k\,(k=3,4,\ldots)$都是右逆

且当$k\neq l$时，可证$v_k\neq v_l$：

反证法：假设$v_k=v_l\Rightarrow v_{k-1}u=v_{l-1}u\Rightarrow v_{k-1}=v_{l-1}$

由归纳假设矛盾

12.D是整环，$D[X]$则也是整环。

证明：

D是整环，$D\neq\{0\}$，故$D[X]\neq\{0\}$

D可交换，显然$D[X]$也可交换

D内无零因子，$\forall f_1(x), f_2(x)\in D[X]^*$，

若$f_1(x)f_2(x)=0$，设$\deg f_1(x)=n\geq 0, \deg f_2(x)=m\geq 0$

$f_1(x)=a_1x^n+\ldots, f_2=b_1x^m+\ldots, a_1\neq 0, b_1\neq 0$

$f_1(x)f_2(x)=a_1b_1x^{n+m}+\ldots\neq 0$矛盾

$\therefore f_1(x)=0$或$f_2(x)=0$

因而$D[X]$中也无零因子。

习题 3.2

1. S 是 A 的子环的充分必要条件是对任意 a,b∈S 有 a-b, ab∈S。

证 必要性：显然。

充分性：对任意 a,b∈S 有 a-b∈S，由群的理论得 （S，+）是子群。

对任意 a,b∈S 有 ab∈S，知 (S,&#0;)是半群。

S 中分配律自然成立。

所以 S 是 A 的子环。

2. S_1，S_2 是 A 的子环，则 $S_1\cap S_2$ 也是子环。S_1+S_2 也是子环吗？

证 由上题子环的充分必要条件，要证对任意 $a,b\in S_1\cap S_2$ 有 a-b, $ab\in S_1\cap S_2$：

因为 S_1，S_2 是 A 的子环，故 a-b, $ab\in S_1$ 和 a-b, $ab\in S_2$ ，

因而 a-b, $ab\in S_1\cap S_2$ ，所以 $S_1\cap S_2$ 是子环。

S_1+S_2 不一定是子环。在矩阵环中很容易找到反例：

设$A=M_2(Z)$, $S_1=\left\{\begin{bmatrix}a&0\\c&0\end{bmatrix}\middle|a,c\in Z\right\}$, $S_2=\left\{\begin{bmatrix}a&b\\0&0\end{bmatrix}\middle|a,b\in Z\right\}$,

易见S_1与S_2均为子环,但$S_1+S_2=\left\{\begin{bmatrix}a&b\\c&0\end{bmatrix}\middle|a,b,c\in Z\right\}$不是子环.

3. H 是 A 的理想的充分必要条件是对任意 a,b∈H, x∈A 有 a-b,ax,xa∈H 。

证 必要性：显然。

充分性：因对任意 a,b∈H 有 a-b, ab∈H, 所以 H 是子环。

又因 ax, xa∈H, 所以 H 是理想。

4. I, J 是 A 的理想，则 I+J, IJ, I∩J 均为理想。

在 (Z, +) 中确定 (m)+(n), (m)(n), (m)∩(n)。

证 对任意 a+u, b+v∈I+J, x∈A 有

(a+u)-(b+v)=(a-b)+(u-v)∈I+J, x(a+u)=xa+xu∈I+J，(a+u)x=ax+ux∈I+J,

所以 I+J 是理想。

对乘法有 IJ={∑au|a∈I, u∈J }。对任意$\sum_1 au$, $\sum_2 au\in IJ$ 有

$\sum_1 au-\sum_2 au=\sum_1 au+\sum_2(-a)u=\sum_3 au\in IJ$,

$x\sum au=\sum(xa)u\in IJ$, $(\sum au)x=\sum a(ux)\in IJ$ 。

所以 IJ 是理想。

类似可证 I∩J 是理想。(略)

(m)+(n)=(d), d=(m,n),

(m)(n)=(mn),

(m)∩(n)=(h), h=[m,n]。

5. 确定 $(Z_n,+)$ 中的所有理想。

解 $(Z_n,+)$ 中的所有理想为

(d), d|n 。其中 d 表示模 n 的同余类。（下同）

详细地可表为：

设 n 的标准素因子分解式为 $n=p_1^{n1}p_2^{n2}...p_s^{ns}$，则$(Z_n,+)$ 中的所有理想为

（$p_1^{i1}p_2^{i2}...p_s^{is}$）, 0≤ik≤nk, 1≤k≤s 。

6. 证明 $M_n(Z)$不是单环，并确定 $M_n(Z)$中所有理想。

证 在本节我们曾证明了数域上的全矩阵环是单环。但整数环不是数域，且有理想：(d), d=0,1,2,... 。因而我们猜想 $M_n(Z)$中全部理想为：

$I(d)=\{(a_{ij})_{n\times n}|a_{ij}\in(d)\}$, d=0,1,2,... 。 （*）

下面我们来证明这一点。

首先，I(d) 显然是理想。

下证 $M_n(Z)$中任何一个理想都是某个 I(d)：

设 J 是 $M_n(Z)$中任何一个理想。令

H={a|a 是矩阵 A∈J 中的元素}，

即 H 是 J 中所有矩阵的元素所构成的集合，因而 H 是 Z 的子集。

可证 H 是(Z,+,•)的一个理想：

对于任何 a_{ij}，$b_{kl}\in H$，则 $E_{ij}A-E_{ik}BE_{lj}\in J$, 经过计算可得 $a_{ij}-b_{kl}\in H$. 其中 E_{ij} 是第 ij 个元素为 1，其余元素为 0 的矩阵。

又，对于任何 a∈H, x∈Z, 有 xA=(xa),Ax=(ax)∈J, 故 xa,ax∈H。所以 H 是 Z 的一个理想。

这就证明了 $M_n(Z)$中全部理想为（*）。

7. L 是 A 的左理想，则 N={x|x∈A, xL=0}是理想。

证 按理想的条件来证。

对任意 a, b∈N, (a-b)L=aL-bL=0, 故 a-b∈N。

对任意 a∈N, x∈A 有 axL=aL=0, xaL=x0=0, 故 ax, xa∈N。

所以 N 是 A 的理想。

8. 设 A 是环，H 是理想，决定 A/n：

（1）A=Z[x], H=(x^2+1)。

解 根据商环的定义，其元素是加群中的陪集，故

A/H= Z[x]/ (x^2+1)={f(x)+H|f(x)∈A}={f(x)+ (x^2+1)| f(x)∈A}

={ax+b+ (x^2+1)|a,b∈Z}={[ax+b]|a,b∈Z}，

其中[ax+b]表示模(x^2+1)的同余类。

进一步可证 Z[x]/ (x^2+1)≌Z[i]。

（2）A=Z[i], H=(2+i)。

解 A/H= Z[i]/ (2+i)={a+bi+(2+i)| a,b∈Z }，

用 [a+bi] 表示 a+bi 的模(2+i)的同余类。则因为 [2+i]=[0], 得 [i]=[-2]，因而对任何 a,b∈Z, [a+bi]=[a-2b], 又因 5=(2+i)(2-i), [5]=[0], 所以全部同余类只有：[0], [1], [2], [3], [4]。故有

Z[i]/ (2+i)={[0], [1], [2], [3], [4]} ≌Z_5 。

(3)$A=\left\{\begin{bmatrix}a&b\\0&c\end{bmatrix}\middle|a,b,c\in Z\right\}$, $H=\left\{\begin{bmatrix}0&2x\\0&0\end{bmatrix}\middle|x\in Z\right\}$

解 由于对任何$\begin{bmatrix}a&b\\0&c\end{bmatrix}\in A$,可表为

$\begin{bmatrix}a&b\\0&c\end{bmatrix}=\begin{bmatrix}a&o\\0&c\end{bmatrix}+\begin{bmatrix}0&2n\\0&0\end{bmatrix}$,当$b=2n$,或

$\begin{bmatrix}a&b\\0&c\end{bmatrix}=\begin{bmatrix}a&1\\0&c\end{bmatrix}+\begin{bmatrix}0&2n\\0&0\end{bmatrix}$,当$b=2n+1$.

所以

$A/H=\left\{\overline{\begin{bmatrix}a&0\\0&c\end{bmatrix}},\overline{\begin{bmatrix}a&1\\0&c\end{bmatrix}}\middle|a,c\in Z\right\}$,其中$\overline{X}$表示$X$模$H$的同余类.

9. F 是数域，则 (x) 是 F[x] 的极大理想，从而 F[x]/(x) 是域。

证 先证 (x) 是极大理想。根据极大理想的定义，首先要证它是真理想：显然 (x)≠(0)，(x)≠F[x]，所以 (x) 是真理想。

其次要证：若有理想 I 真包含 (x)，则必有 I=F[x]。

因为 I 真包含 (x)，则存在 f(x)∈I\(x) , $f(x)=a_0+a_1x+...+a_nx^n$, 且 $a_0\neq0$ 。

由此可得 $a_0=f(x)-x(a_1+...+a_nx^{n-1})\in I$, 因而 $a_0a_0^{-1}=1\in I$ ，故 I=F[x]。

所以 (x) 是极大理想。

再由本节定理 1 知 F[x]/(x) 是域。

10. 设 D 为有单位元的环，则 D 为除环的充分必要条件是 D 没有非平凡左理想。

证 复习除环的定义。

必要性：设 I 为非 0 左理想，则存在 $a\neq 0, a\in I$。因 I 是左理想，取 $a^{-1}\in D$ 得

$a^{-1}a=1\in I$，因而 I=D 。所以 D 中没有非平凡左理想。

充分性：已知 D 没有非平凡左理想，要证 D 是除环。

任取 $a\in D$ 且 $a\neq 0$，则 Da 是一个左理想（为什么？），因 $a\in Da$，$Da\neq 0$，由于 D 没有非平凡左理想，故必有 Da=D，于是存在 $b\in D$ 使 ba=1，a 有左逆元，由此可得 $D\setminus\{0\}$是群，所以 D 是除环。

11. R 是可换环，H 是理想，且 $H\neq R$，则 H 是素理想的充分必要条件是 R/H 是整环。

证 素理想的概念不易记忆，可与素数的概念相比较，形式上有某种类似性：

素数：对任何 $a, b\in Z^+$，若 p=ab，则有 p|a 或 p|b 。

素理想：对任何 $a, b\in R$，若 $ab\in H$，则有 $a\in H$ 或 $b\in H$ 。

必要性：已知 H 是素理想，要证 $R/H=\{a+H|a\in R\}$是整环。

设 $a\in R$，用[a]=a+H 表示 R/H 中的元素（模 H 的同余类）。若有 $a, b\in R$ 满足 [a][b]=[0]。由于[a][b]=(a+H)(b+H)=ab+H=[0]=H，故得 $ab\in H$。由于 H 是素理想，得 $a\in H$ 或 $b\in H$，因而有 [a]=[0] 或 [b]=[0]，所以 R/H 是整环。

充分性：已知 R/H 是整环，要证 H 是素理想。

设 $ab\in H$，则[a][b]=[0]，因 R/H 是整环，故有[a]=[0]或[b]=[0]，即 $a\in H$ 或 $b\in H$，所以 H 是素理想。

习题 3.3

1. 设 f 是环 A 到 A' 的同态，证明

（1）f 将 A 中的 0 元映成 A' 中的 0' 元。

（2）f 将 A 中的子环映成 A' 中的子环。

（3）f 将 A 中的理想映成 f(A) 中的理想。

证 （1）由同态定义，f(0)=f(0+0)=f(0)+f(0)，所以 f(0)=0' 。

（2）设 H 是子环，对于任意 $f(h_1), f(h_2)\in f(H)$ 有

$f(h_1)-f(h_2)= f(h_1-h_2)\in f(H)$,

$f(h_1)f(h_2)= f(h_1h_2)\in f(H)$,

所以 f(H)是子环。

（3）设 I 是 A 的理想，由(2)得 f(I)是子环。

对于任意 $f(a)\in f(I)$，$f(x)\in f(A)$ 有

$f(x)f(a)=f(xa)=f(a_1)\in f(I)$,

$f(a)f(x)=f(ax)=f(a_2)\in f(I)$,

所以 f(I)是 f(A)的理想。

2. 设 f 是 A 到 A' 的同态，$a\in A$, b=f(a)，则 $f^{-1}(b)=a+\ker(f)$ 。

证 采用互相包含的证法。

由于 f(a+kerf)=f(a)+0'=f(a)=b，所以 a+kerf 属于 $f^{-1}(b)$。

反之，对任何 $x\in f^{-1}(b)$, f(x)=b=f(a)，得 f(x-a)=0'，所以

$x-a\in$ kerf，即 $x\in$ a+kerf，因而 $f^{-1}(b)$ 属于 a+kerf 。

综上，得 $f^{-1}(b)=a+\ker(f)$ 。

3. 证明本节定理 1 至定理 4。

参考群论里类似的定理的证明，注意环与群的不同。

4. 利用同态基本定理证明

（1）$R[x]/(x^2+1)\cong(C,+,\cdot)$。

（2）F[x]/(x)≌F，F 为数域。

（3）$Z[i]/(3+i)\cong(Z_{10},+,\cdot)$。

证 （1）作映射 φ：f(x)→f(i)(R[x] →C)，

由于 $\varphi(f_1(x)+f_2(x))= f_1(i)+f_2(i)= \varphi(f_1(x))+ \varphi(f_2(x))$,

$\varphi(f_1(x)f_2(x))= f_1(i)f_2(i)= \varphi(f_1(x))\varphi(f_2(x))$,

故 φ 是同态，对任意 $a+bi\in C$，取 f(x)=a+bx，则 φ(f(x))=a+bi，因而 φ 是满同态。

求核：$\ker\varphi=\{f(x)\in R[x]|f(i)=0\}=\{f(x)\in R[x]|(x-i)|f(x)\}$

$=\{f(x)\in R[x]|(x^2+1)|f(x)\}=(x^2+1)$。

所以由同态基本定理得

$R[x]/(x^2+1)\cong(C,+,\cdot)$。

（2）作映射 φ：f(x)→f(0)(F[x] →F)，

由于 $\varphi(f_1(x)+f_2(x))= f_1(0)+f_2(0)= \varphi(f_1(x))+ \varphi(f_2(x))$,

$\varphi(f_1(x)f_2(x))= f_1(0)f_2(0)= \varphi(f_1(x))\varphi(f_2(x))$,

故 φ 是同态，对任意 $a\in C$，取 f(x)=a，则 φ(f(x))=a，因而 φ 是满同态。

求核：$\ker\varphi=\{f(x)\in F[x]|f(0)=0\}=\{f(x)\in F[x]|x|f(x)\}=(x)$,

所以由同态基本定理得

$F[x]/(x)\cong(F,+,\cdot)$。

（3）对此题同态映射并不明显，所以我们首先要确定同态映射。

设 $Z_{10}=\{[0],[1],[2],...,[9]\}$，其中[k]表示 k 模 10 的同余类。

设 φ 是 Z[i]到 Z_{10} 的非零同态映射，则可设 φ(1)=[1]，φ(i)=[k]，则由

$\varphi(i^2)= \varphi(-1)=[k]^2=-[1]$，得 $k^2+1\equiv 0(\mathrm{mod}10)$。取 k=-3，则得

φ(a+bi)=[a-3b].

下面证明 φ 是同态：

φ((a+bi)(c+di))= φ(ac-bd+(ad+bc)i)=[ac-bd-3(ad+bc)],

φ(a+bi)φ(c+di))=[a-3b][c-3d]=[ac+9bd-3(ad+bc)]=[ac-bd-3(ad+bc)],

所以 φ((a+bi)(c+di))= φ(a+bi)φ(c+di))。

类似可证 φ((a+bi+c+di))= φ(a+bi)+φ(c+di))。

因而 φ 是同态，且易证是满同态。

求核：$\ker\varphi=\{a+bi|[a-3b]=[0]\}=\{(3+i)b+10q|b,q\in Z\}$

$=\{(3+i)b+(3+i)(3-i)q|\ b,q\in Z\}$

$=\{(3+i)x|x\in Z[i]\}=(3+i)$,

所以由同态基本定理得

$Z[i]/(3+i)\cong(Z_{10},+,\cdot)$。

5. 将复数环同构嵌入 $M_2(R)$ 中.

解 首先要找一个$(C,+,\cdot)$到$M_2(R)$的同构映射.

设 f 是$(C,+,\cdot)$到$M_2(R)$的同构映射,由 $f(1)=\begin{bmatrix}1&0\\0&1\end{bmatrix}$,

得 $f(a)=\begin{bmatrix}a&0\\0&a\end{bmatrix}$, $\forall a\in R$.由于 i 是 C 中的二阶元可令

$f(i)=\begin{bmatrix}0&1\\-1&0\end{bmatrix}$,于是得

$$f(a+bi)=\begin{bmatrix}a&b\\-b&a\end{bmatrix},(C\to M_2(R)).$$

不难验证 f 是同态,且是单同态,所以 f 把 C 嵌入$M_2(R)$.

4. 将复数环同构嵌入

6. 找出 (Z_n,+,&#0;)上一切自同态。

解 解决这类问题通常是根据同态定义找出一些特殊元素，例如单

位元，生成元等的象，再找出一般元素的象，从而确定所有同态映射。方法类似于本节例 4。

设 Z={[0],[1],...,[n-1]}，其中[k]表示 k 模 n 的同余类。

设 f 是(Z_n,+,&#0;)上任一自同态，可设 f([1])=[k]，则对任意[x]∈Z_n 有 f([x])=[kx]。

由 f([1])=f([1]&#0;[1])得 [k]=$[k]^2$，有解：[k]=[0]或[1]。因而(Z_n,+,&#0;)上全部自同态有：

f([x])=[kx]，对任何[x]∈Z_n。其中[k]满足方程 [k]([k]-1)=[0]，或 k(k-1)=0(modn)。

7. A={(a_1, a_2, ... a_n)|a_i∈Z}对向量的加法构成群，E(A)为 A 上的自同态环，证明

E(A)≌M_n(Z)。

证 首先要确定 E(A)。

设 f 为 A 上的任一自同态。由于

对任意 α, β ∈A 有 f(α+β)=f(α)+f(β),

对任意 k 有 f(kα)=kf(α),

所以 f 是 A 上的线性变换，因而有

f(α)=Bα, B∈M_n(Z)。

反之，对任意 B∈M_n(Z), 定义 A 上的变换 f_B 为

f_B(α)=Bα。

则不难证明 f_B 是 A 上的自同态环。

下证 E(A)≌M_n(Z)：

作映射 σ：f_B→B (E(A) →M_n(Z))，其中 f_B(α)=Bα。

由于 σ(f_B+ f_C)=B+C=σ(f_B)+ σ(f_C),

σ($f_B f_C$)=BC=σ(f_B)σ(f_C),

故 σ 是同态。易见是满同态，

不难证明 σ 是双射，因而 σ 是同构。

所以 E(A)≌M_n(Z)。

8. m,r∈Z^+, r|m, Z_m={[0],[1],...,[m-1]}, Z_r={0,1,...,r-1}，均为同余类环。证明

f:[a]→a 是 Z_m 到 Z_r 的同态，并求 kerf, Z_m/kerf。

证 首先要验证一下 f 是映射，因为如果对一般的 m,r，这样的 f 不一定是映射。

由于 [a]=[b] => [a-b]=[0] => m|(a-b) => r|(a-b) => a=b，故 f 是映射。

再证是同态映射：

f([a]+[b])=f([a+b])=a+b=f([a])+f([b]),

f([a][b])=f([ab])=ab=f([a])f([b]),

故 f 是同态，且显然是满同态。

求核：

kerf={[a]|a=0}={[0],[r],[2r],...,[m-r]}.

所以由同态基本定理得

Z_m/kerf≌Z_r。

9. 证明 $AutZ[x] \cong \left\{ \begin{bmatrix} 1 & b \\ 0 & \varepsilon \end{bmatrix} \middle| \varepsilon = \pm 1, b \in Z \right\}$

证 首先要求 $AutZ[x]$ 的表达式.方法类似于前面求所有自同态(构)的方法.

设 σ 为 $Z[x]$ 上任一自同构,由于 $Z[x]=(1,x)$,必有 $\sigma(1)=1, \sigma(x)=ax+b$.

(注意这一步是来之不易的,需要论证.)

由 σ 是满射可推出 $a=\pm 1$,因而 σ 可表为 $\sigma_{\varepsilon,b}(x)=\varepsilon x+b$.这样,可进一步表为

$\sigma_{\varepsilon,b}(f(x))=f(\varepsilon x+b)$,

故得

$AutZ[x]=\{\sigma_{\varepsilon,b} \mid \varepsilon=\pm 1, b \in Z, \sigma_{\varepsilon,b}(f(x))=f(\varepsilon x+b)\}$.

下面证明与右边的矩阵群同构.

作映射 $\varphi: \sigma_{\varepsilon,b} \mapsto \begin{bmatrix} 1 & b \\ 0 & \varepsilon \end{bmatrix} (AutZ[x] \to G)$,

为证明 $\varphi(\sigma_{\varepsilon,b}\sigma_{\eta,c})=\varphi(\sigma_{\varepsilon,b})\varphi(\sigma_{\eta,c})$,需先证明 $\sigma_{\varepsilon,b}\sigma_{\eta,c}=\sigma_{\varepsilon\eta,\eta b+c}$.

φ 显然是双射,所以得证.

10. 求 Z[i], Z[x], 偶数环的分式域。

解 主要熟悉一下分式域的概念。

由分式域的定义，可得

P(Z[i])={(a+bi)/(c+di)|a,b,c,d∈Z, cd≠0}={q+si|q,s∈Q}=Q[i].

P(Z[x])={f(x)/q(x)|f(x),q(x) ∈ Z[x],q ≠ 0}={f(x)/q(x)|f(x),q(x) ∈ Q[x],q≠0}

=P(Q[x]).

P(偶数环)=Q。

习题 3.4

1. 证明相伴关系是等价关系，并满足：a∽b, c∽d => ac∽bd。

证 先证相伴关系∽是等价关系：

反身性：因 a|a，故 a∽a；

对称性：a∽b => a|b 且 b|a => b∽a；

传递性：a∽b 且 b∽c => a|b, b|a 且 b|c, c|b => a|c, c|a => a∽c。

再证对乘法保持运算：

a∽b, c∽d => a|b, b|a, c|d, d|c => ac|bd, bd|ac => ac∽bd。

2. 叙述两个元素的最小公倍元的定义，并将最大公因子与最小公倍元的定义推广到多个元素。

答 复习最大公因子的定义，类似可得最小公倍元的定义：

定义 设 D 是有单位元的整环，a, b∈D。若有 m∈D 满足：

（1）a|m, b|m；

（2）若有 m' 满足 a|m', b|m'，则 m|m'。

则称 m 是 a 与 b 的最小公倍元，并记作 m∽[a,b]。

多个元素的情形：

定义 设 D 是有单位元的整环，a, b, ..., h∈D。若有 m∈D 满足：

（1）a|m, b|m, ..., h|m；

（2）若有 m' 满足 a|m', b|m',..., h|m'，则 m|m'。

则称 m 是 a,b,...,h 的最小公倍元，并记作 m∽[a,b,...,h]。

定义 设 D 是有单位元的整环，a, b, ..., h∈D。若有 v∈D 满足：

（1）v|a, v|b, ..., v|h；

（2）若有 v' 满足 v'|a, v'|b,..., v'|h，则 v'|v。

则称 v 是 a,b,...,h 的最大公因子，并记作 m∽（a,b,...,h）。

3. 设 p 为既约元，则 (p) 为非平凡理想。

证 要证 (p)≠{0} 和 (p)≠D。

因为 p≠0，故 (p)≠{0}。

再证(p)≠D 。反证法：假设 (p)=D ,则存在 q∈D 使 pq=1，因而 p 是可逆元，这与 p 是既约元矛盾。

4. 在$Z[\sqrt{-5}]$中下列元素哪些是既约元？$2,7,29,2-\sqrt{-5},6+\sqrt{-5}$.

解 首先我们研究$Z[\sqrt{-5}]$中既约元的条件.可以证明以下两个定理：

定理1 设p为素数,则p为既约元的充分必要条件是$p\neq a^2+5b^2,\forall a,b\in Z$.

定理2 设$\alpha=a+b\sqrt{-5},(a,b)=1$.则当$v(\alpha)=a^2+5b^2=$素数或$v(\alpha)<36$时$\alpha$是既约元.

根据定理1, 2,7是既约元;29不是既约元,事实上,$29=(3+2\sqrt{-5})(3-2\sqrt{-5})$.

根据定理2, $v(2-\sqrt{-5})=9<36$,所以$2-\sqrt{-5}$是既约元.

$v(6+\sqrt{-5})=41=$素数,所以$6+\sqrt{-5}$也是既约元.

5. 设 D 为有单位元的整环，则 p 是素元的充分必要条件是 D/(p)是整环。

证 复习素元的定义。

必要性：已知 p 是素元。要证 D/(p) 是整环，一是要证 D/(p)≠0；二是要证 D/(p)中无零因子。

由本节习题 3，(p)为非平凡理想，故 D/(p)≠0 。

对任何 [a],[b]∈D/(p)，若 [a][b]=[0]，则 ab∈(p)，可设 ab=pq，故 p|ab，由于 p 是素元，必有 p|a 或 p|b，故有 [a]=[0] 或[b]=[0]。这就证明了 D/(p)中无零因子。

所以 D/(p)是整环。

充分性：已知 D/(p)是整环，要证 p 是素元。

设 p|ab，则 [ab]=[0]，由于 D/(p)是整环，必有 [a]=[0] 或[b]=[0]，可得 p|a 或 p|b，所以 p 是素元。

6. $\alpha=a+bi\in Z[i]$, $v(\alpha)=a^2+b^2=$素数，证明α是 Z[i]中的既约元。

证 复习既约元的定义。

设$\alpha=\beta\gamma$，则 $v(\alpha)=v(\beta)v(\gamma)$，由于 $v(\alpha)=a^2+b^2=$素数，

必有 $v(\beta)=1$ 或 $v(\gamma)=1$，即 $\beta\in U(Z[i])$ 或 $\gamma\in U(Z[i])$。

所以α是 Z[i]中的既约元。

习题 3.5

利用 3.5 节定理 2 证明域上的多项式环 F[x]是唯一分解环。

证 复习该定理。要证以下两点：

（1）证明 F[x]中任一真因子序列含有限项。

设 f(x)为 F[x]中 degf(x)=n>0 的任一多项式，若 g(x)是 f(x)的真因子，则 deg(g(x))<n。由于小于 n 的正整数只有有限个，而对应多项式真因子序列的正整数序列是一个严格减序列，所含的整数必只有有限个，所以，f(x)的多项式真因子序列也只有有限个。

（2）F[x]中任意两个非零多项式都有最大公因子。在高等代数中我们单独证明了数域上任意两个非零多项式都有最大公因子。

综上，F[x]是唯一分解环。

2. 证明 Z[√-5]满足定理 2 条件Ⅰ。

证 定理 2 条件Ⅰ：任一真因子序列含有限项。

任取一个元素$\alpha=a+b\sqrt{-5}$，则 $v(\alpha)=a^2+5b^2\in Z^+$，设$\alpha_1$是α的真因子，则 $v(\alpha_1)<v(\alpha)$,类似，若α_2是α_1的真因子，则 $v(\alpha_2)<v(\alpha_1)$,...。由于小于 v(α)的整数只有有限个，所以，α的真因子序列含有限项。

3. 证明 Z[√10]不是唯一分解环。

证 利用定理 2 条件Ⅱ：任一既约元都是素元。

考虑元素 3，显然是既约元。

由于 3|(1+√10)(1-√10)，但 3 不能整除(1+√10)，也不能整除(1-√10)。故 3 不是素元，所以 Z[√10]不是唯一分解环。

3. 证明在唯一分解环中,$ab\sim(a,b)[a,b]$.

证 利用元素的素因子分解式.

设a,b的素因子分解式为

$$a=p_1^{r_1}p_2^{r_2}\cdots p_s^{r_s},\quad r_i\geq 0.$$

$$b=p_1^{t_1}p_2^{t_2}\cdots p_s^{t_s},\quad t_i\geq 0.$$

取 $m_i=\min(r_i,t_i),\quad n_i=\max(r_i,t_i),\quad i=1,2,\cdots,s.$

则 $(a,b)\sim p_1^{m_1}p_2^{m_2}\cdots p_s^{m_s}$,

$[a,b]\sim p_1^{n_1}p_2^{n_2}\cdots p_s^{n_s}$,

且有 $m_i+n_i=r_i+t_i,\quad i=1,2,\cdots,s.$

所以

$$(a,b)[a,b]\sim ab.$$

5. 下列环是否是欧氏环,并证明之.

该题的关键是对每一个环找到一个范数$v(\alpha)$的定义,要求满足$v(\alpha)>0,\forall\alpha\neq 0$.一般还要求满足$v(\alpha\beta)=v(\alpha)(\beta)$.最重要的是能进行欧氏除法.

如果找不到这样的的范数,则可猜想它不是欧氏环.要证明它不是欧氏环,通常证明它不是唯一分解环.可以通过找到一个既约元不是素元,或找到两个元素无最大公因子.

(1) $Z[\sqrt{2}]=\{a+b\sqrt{2}\mid a,b\in Z\}$

解 $\forall\alpha=a+b\sqrt{2}\in Z[\sqrt{2}]$,令$v(\alpha)=|a^2-2b^2|$,则不难验证: $v(\alpha)(\beta)=v(\alpha)v(\beta)$.

下证满足欧氏除法的要求.

$\forall\alpha=a+b\sqrt{2}\neq 0$, $\beta=c+d\sqrt{2}$, 令$q=u+v\sqrt{2}$,则由$\beta=q\alpha+r$,可得

$$r=\alpha\left[\left(\frac{ac-2bd}{a^2-2b^2}-u\right)+\left(\frac{ad-bc}{a^2-2b^2}-v\right)\sqrt{2}\right],$$

可选适当的u,v使 $\left|\frac{ac-2bd}{a^2-2b^2}-u\right|\leq\frac{1}{2},\left|\frac{ad-bc}{a^2-2b^2}-v\right|\leq\frac{1}{2}.$

因而可得 $r=0$或$v(r)=v(\alpha)v\left[\left(\frac{ac-2bd}{a^2-2b^2}-u\right)+\left(\frac{ad-bc}{a^2-2b^2}-v\right)\sqrt{2}\right]$

$$\leq v(\alpha)(\frac{1}{4}+\frac{2}{4})<v(\alpha).$$

所以$Z[\sqrt{2}]$是欧氏环.

(2) $Z[\sqrt{-2}]=\{a+b\sqrt{-2}\mid a,b\in Z\}$

解 方法类似(1).

$\forall\alpha=a+b\sqrt{-2}\in Z[\sqrt{-2}]$,令$v(\alpha)=a^2+2b^2$,则不难验证: $v(\alpha)(\beta)=v(\alpha)v(\beta)$.

下证满足欧氏除法的要求.

$\forall\alpha=a+b\sqrt{-2}\neq 0$, $\beta=c+d\sqrt{-2}$, 令$q=u+v\sqrt{-2}$,则由$\beta=q\alpha+r$,可得

$$r=\alpha\left[\left(\frac{ac+2bd}{a^2+2b^2}-u\right)+\left(\frac{ad-bc}{a^2+2b^2}-v\right)\sqrt{-2}\right],$$

可选适当的u,v使 $\left|\frac{ac+2bd}{a^2+2b^2}-u\right|\leq\frac{1}{2},\left|\frac{ad-bc}{a^2+2b^2}-v\right|\leq\frac{1}{2}.$

因而可得 $r=0$或$v(r)=v(\alpha)v\left[\left(\frac{ac+2bd}{a^2+2b^2}-u\right)+\left(\frac{ad-bc}{a^2+2b^2}-v\right)\sqrt{-2}\right]$

$$\leq v(\alpha)(\frac{1}{4}+\frac{2}{4})<v(\alpha).$$

所以$Z[\sqrt{-2}]$是欧氏环.

(3) $Z[\sqrt{-3}]=\{a+b\sqrt{-3}|a,b\in Z\}$

解 如果用类似(2)的方法,定义$v(\alpha)=|a^2+3b^2|$,一直可进行下去,但最后只能得到$v(r)\le v(\alpha)$,而不是严格不等式因而我们猜想它不是欧氏环.

考虑元素4,它可分解为 $4=2\cdot 2=(1+\sqrt{-3})(1-\sqrt{-3})$,其中$2,1+\sqrt{-3},1-\sqrt{-3}$都是既约元,即4有两种不等价的既约元分解式,所以$z[\sqrt{-3}]$不是唯一分解环,因而也不是欧氏环.

(4) $D=\{a+b\sqrt{-3}|a,b$同时为整数,或同时为奇数的$\frac{1}{2}\}$

解 该题初看似乎与(3)类似,但由于a,b的取值范围有了扩大,我们首先从正面来证明.

$\forall\alpha=a+b\sqrt{-2}\in D$,令$v(\alpha)=a^2+3b^2$,则不难验证: $v(\alpha\beta)=v(\alpha)v(\beta)$.

下证满足欧氏除法的要求.

$\forall\alpha=a+b\sqrt{-3}\ne 0,\ \beta=c+d\sqrt{-3}$,令$q=u+v\sqrt{-3}$,则由$\beta=q\alpha+r$,可得

$$r=\alpha\left[\left(\frac{ac+3bd}{a^2+3b^2}-u\right)+\left(\frac{ad-bc}{a^2+3b^2}-v\right)\sqrt{-3}\right],$$

由于u,v同时为整数,或同时为奇数的$\frac{1}{2}$,可选适当的u使 $\left|\frac{ac+3bd}{a^2+3b^2}-u\right|\le\frac{1}{4}$,(为什么?)

当u选定后,总可选适当的与u同一类型的数使$\left|\frac{ad-bc}{a^2+2b^2}-v\right|\le\frac{1}{2}$.

因而可得 $r=0$或$v(r)=v(\alpha)v\left[\left(\frac{ac+3bd}{a^2+3b^2}-u\right)+\left(\frac{ad-bc}{a^2+3b^2}-v\right)\sqrt{-3}\right]\le v(\alpha)\left(\frac{1}{16}+\frac{3}{4}\right)<v(\alpha)$,

所以D是欧氏环.

6. p 为奇素数,a≠0(mod p),则 x^2=a(mod p) 在 Z 中有解的充分必要条件是

$a^{(p-1)/2}$=1(mod p) 。并由此证明当 p 为形如 4n+1(n∈Z^+) 的素数时,p 不是 Z[i] 中的素元。

证 熟悉同余式的意义。

必要性:设 x^2=a(mod p) 在 Z 中有解,其解为 x=b 。则有

a=b^2 (mod p),因而 $a^{(p-1)}$/2=b^{p-1} (mod p) 。

由 a≠0(mod p),得 b≠0(mod p) 。故 [b]∈Z^*_p 。考虑乘群 (Z^*_p,&#0;) 的阶为 p-1 ,故有 $[b]^{(p-1)}$=[1] ,即 b^{p-1}=1(mod p),所以 $a^{(p-1)/2}$=1(mod p) 。

充分性:设 a 满足 $a^{(p-1)/2}$=1(mod p) ,要证 x^2=a(mod p) 在 Z 中有解。

考虑多项式 f(x)=$x^{(p-1)/2}$-1∈Z_p[x], [a]是它的一个根。可以看出 [1^2], [2^2], ..., $[(p-1)/2]^2$ 都是 f(x) 的根。且可证这些根互不相同:[a^2]=[b^2] => [a^2-b^2]=[0] => p|(a-b)(a+b),由于 0<a,b≤(p-1)/2,故有 0<a+b≤p-1,因而 (p,a+b)=1,得 p|(a-b). 又由于 |a-b|≤(p-1)/2,所以 a=b.

这就是说[1^2], [2^2], ..., $[(p-1)/2]^2$ 是 f(x) 的全部根。因而必有某个 c 使

[a]=[c^2],即 c^2=a(mod p),所以方程 x^2=a(mod p) 在 Z 中有解。

最后,设 p=4n+1,考虑方程 x^2=-1(mod p)。由于 $(-1)^{(p-1)/2}$=$(-1)^{2n}$=1(mod p),由刚证明的结论,方程 x^2= -1(mod p)在 Z 中有解,设其解为 u,则得 u^2= -1(mod p),即 u^2+1=0(mod p)。

现在环 Z[i]中考虑 u^2+1=0(mod p),得 p|(u^2+1) => p| (u-i)(u+i),由于 p 既不能整除(u-i),也不能整除(u+i),所以 p 不是素元。

7. 设 p 是素数,则 p 是 Z[i]中的素元的充分必要条件是 p≡3(mod4)。

证 必要性:由习题 6。

充分性:已知 p≡3(mod4),要证 p 是 Z[i]中的素元。

反证法。假设 p 不是 Z[i]中的素元,因而也不是既约元,p 有真分解式:p=αβ,α,β∈Z[i],且α,β都不是可逆元。

设 v(α)是α的范数,则有 v(p)=P^2=v(α)v(β),v(α),v(β)∈Z,由于 v(α),v(β)>1,必有 v(α)=v(β)=p 。令α=a+bi,得 p=a^2+b^2,由于(a,b)=1(否则 a^2+b^2不是素数),因而 a 与 b 的奇偶性相反,所以 p=a^2+b^2=$(2n)^2$+$(2k+1)^2$=1(mod4),矛盾。

习题 3.6

1.证明$Z[x]$不是主理想整环.

证 证明思路:方法1.根据主理想整环的定义,在$Z[x]$中找一个理想不是主理想.这样的理想有什么特点呢?我们可取$u(x),v(x)\in Z[x]$,使$I=(u(x),v(x))\ne Z[x]$,但$u(x)$与$v(x)$的最大公因子为本1.这样的多项式容易找到.

方法2.利用主理想整环的最大公因子定理(本节定理4推论1),用反证法.

方法3.利用主理想整环的性质(本节定理4推论2):取即约元x,用反证法.

我们用方法1.取理想$I=(2,x)$.下面证明I不是主理想.

反证法:假设I是主理想,并设$I=(2,x)=(f(x))$,则$f(x)|2$和$f(x)|x$,易得$f(x)\sim 1$,

则$(f(x))=(1)=Z[x]$.但可证$1\notin(2,x)$,否则存在$u(x),v(x)\in Z[x]$使$2u(x)+xv(x)=1$,设 $u(x)=a_0+a_1x+\cdots$,得$2a_0=1$,而a_0在Z中无解.所以I不是主理想.

其它方法留给读者.

2.设D是唯一分解环,P是D的分式域,证明

(1) $f(x)\in P[x]$,则$f(x)$可表为$f(x)=r\varphi(x)$,其中$r\in P$, $\varphi(x)\in D[x]$是$D[x]$上的本原多项式.

(2) $f(x)\in D[x]$,若$f(x)$在$D[x]$上不可约,则$f(x)$在$P[x]$上也不可约.

(3) $f(x)\in D[x]$是首1多项式, $g(x)$是$f(x)$在$P[x]$中的首1多项式因子,则$g(x)\in D[x]$.

证 本题熟悉本原多项式和分式域的概念.

(1)设$f(x)=r_0+r_1x+\cdots+r_nx^n, r_i\in P$.

由于P是D的分式域,r_i可表为$r_i=a_i^{-1}b_i, a_i,b_i\in D, i=0,1,\cdots,n$.

于是$f(x)$可表为

$$f(x)=\frac{1}{a_0a_1\cdots a_n}\left(b_0q_0+b_1q_1x+\cdots+b_nq_nx^n\right),$$

令$d=(b_0q_0,b_1q_1,\cdots,b_nq_n)$,则

$$f(x)=\frac{d}{s}\left(p_0+p_1x+\cdots+p_nx^n\right),\text{其中}d,s,p_i\in D,(p_0,p_1,\cdots,p_n)=1.$$

令$r=\frac{d}{s}$, $\varphi(x)=(p_0+p_1x+\cdots+p_nx^n)$,则

$f(x)=r\varphi(x), r\in P, \varphi(x)\in D[x]$是$D[x]$上的本原多项式.

(2) $f(x)\in D[x]$,若$f(x)$在$D[x]$上不可约,则$f(x)$在$P[x]$上也不可约.

反证法. 假设$f(x)$在$P[x]$上可约, $f(x)$可表为$f(x)=g(x)h(x), g(x),h(x)\in P[x]$, $\deg g(x)\ge 1, \deg h(x)\ge 1$由(1), $g(x),h(x)$可表为$g(x)=r\varphi(x), h(x)=s\psi(x)$,其中 $r,s\in P$, $\varphi(x),\psi(x)\in D[x]$是本原多项式且$\deg\varphi(x)\ge 1$和$\deg\psi(x)\ge 1$.于是得

$f(x)=rs\varphi(x)\psi(x)$,

另一方面, $f(x)$也可表为

$f(x)=d\delta(x)$,其中$d\in D, \delta(x)\in D[x]$是本原多项式.

由本节中性质(2)和(3)高斯引理,得$rs\sim d, \varphi(x)\psi(x)\sim\delta(x)$,因而有

$f(x)=ud\varphi(x)\psi(x)$,

这与$f(x)$在$D[x]$上不可约矛盾.

(3) $f(x)\in D[x]$是首1多项式, $g(x)$是$f(x)$在$P[x]$中的首1多项式因子,则$g(x)\in D[x]$.

设 $f(x)=g(x)h(x), h(x)\in P[x]$,则$h(x)$也是首1多项式,由(1),可设

$g(x)=\frac{r}{s}\varphi(x), h(x)=\frac{t}{u}\psi(x), r,s,t,u\in D$, $\varphi(x),\psi(x)\in D[x]$是本原多项式.

于是得 $f(x)=\frac{rt}{su}\varphi(x)\psi(x)$,由高斯引理和唯一性,得$\frac{rt}{su}\sim 1$($D$中),因而$\frac{r}{s}\sim 1, \frac{t}{u}\sim 1$,

所以$g(x)\in D[x]$.

3. 若D是有单位元的整环但不是域,则$D[x]$不是主理想整环.

证　复习主理想整环的概念和性质.是本节第1题的推广.
要证$D[x]$不是主理想整环,最直接的方法是找一个理想不是主理想.

由于D不是域,存在元素$a \in D \setminus U(D)$,作理想$I = (a, x)$,显然,$I \neq (0)$和$I \neq D[x]$(因为$1 \notin I$).

下证I不是主理想.反证法.假设I是主理想并设$I = (a, x) = (f(x)), f(x) \in D[x]$.
则得$f(x) \mid a$,因而$f(x) = q \in D$,又$f(x) \mid x$,即$q \mid x$,因而$q \sim 1$,于是有$I = (1) = D[x]$,矛盾.
故I不是主理想.

所以$D[x]$不是主理想整环.

4. 判断下列多项式在$Q[x]$上是否可约?

(1)$x^4 + 1$.

解　作变换,再利用$Eisenstein$定理.

令$f(x) = x^4 + 1$,则

$f(x+1) = x^4 + 4x^3 + 6x^2 + 4x + 2$,

由$Eisenstein$定理,取$p = 2$,知$f(x+1)$在$Q[x]$上不可约,所以

$f(x)$在$Q[x]$上也不可约.

(2)$x^2 + px + 1$, p为素数.

解　令$f(x) = x^2 + px + 1$,分两种情况讨论:

$p = 2$,则$f(x) = x^2 + 2x + 1 = (x+1)^2$,所以$f(x)$在$Q[x]$上不可约.

$p > 2$,考虑$f(x-1) = (x-1)^p + p(x-1) + 1 = x^p - px^{p-1} + \frac{p(p-1)}{2!}x^{p-2} + \cdots + 2px - p$,

由$Eisenstein$定理,知$f(x-1)$在$Q[x]$上不可约,所以$f(x)$在$Q[x]$上不可约.

(3)$x^5 + x^3 + 3x^2 - x + 1$.

令$f(x) = x^5 + x^3 + 3x^2 - x + 1$,作变换,再利用$Eisenstein$定理,均未获成功.

在无更好的路的情况下,只好最后一招:分解因式法.

首先判断是否有一次因式:用1和-1代入,均非根,故在$Q[x]$上无一次因式.

再看能否分解为二次和三次因式之积设

$f(x) = (x^3 + ax^2 + bx + c)(x^2 + dx + e), a, b, c, d, e \in Z$.

得　$a + d = 0, ce = 1, ad + b + e = 1, ae + bd + c = 3, be + cd = -1$.

得　$d = -a, c = e = 1$或$c = e = -1$.

当$c = e = 1$时,有$-a^2 + b = 0, a - ab = 2, b - a = -1$.在$Z$上无解.

当$c = e = -1$时,有$-a^2 + b = 2, -a - ab = 4, b - a = 1$,在$Z$上无解.

所以$f(x)$在$Q[x]$上不可约.

5. 写出$Z_3[x]$中全部次数≤ 3的首1不可约多项式.

解　分次枚举.

1次:　$x, x+1, x+2$;

2次:　x^2+1, x^2+x+2, x^2+2x+2;

3次:　$x^3+2x+1, x^3+2x+2, x^3+2x^2+1, x^3+x^2+1$,

$x^3+x^2+x+2, x^3+x^2+2x+1, x^3+2x^2+x+1, x^3+2x^2+2x+2$.

共14个.

其个数有公式可以计算,参看后面4.3节.

习题 3.7（第一题见最后）

2. 检验下列接收到的码词是否正确？生成多项式为 p(x)=1+x2+x3+x4.

10011011, (2) 01110010, (3) 10110101 .

解 (1) u(x)=1+ x3+x4+x6+x7, p(x)不能整除 u(x)，故有错。

u(x)=x+ x2+x3+x6, p(x)能整除 u(x)，故正确。

u(x)=1+ x2+x3+x5+x7, p(x)不能整除 u(x)，故有错。

第 4 章 习题 4.1 第 1 题解答

1. 设F是域,$chF = p$(素数),$a, b \in F$,证明

(1)$na = mb (a \neq 0) \Rightarrow n \equiv m (\mathrm{mod}\ p)$.

(2),$e \geq 0$整数.

证　熟悉特征为p的域内的运算特性.

(1)$na = mb (a \neq 0)$,由消去律得$n \cdot 1 = m \cdot 1$,(注意这里不能得到$n = m$),

于是有$(n - m) \cdot 1 = 0$,因为$o^+(1) = p$(指1在加法群$(F, +)$中的阶).

故$p \mid (n - m)$,所以$n \equiv m (\mathrm{mod}\ p)$.

(2)对e作归纳法.

$e = 0$,显然公式成立.

$e = 1, (a \pm b)^p = a^p \pm pa^{p-1}b + \cdots + (-1)^k \frac{p(p-1)\cdots(p-k+1)}{k!} a^{p-k}b^k + \cdots \pm b^p$,

由于$(k!) \mid p(p-1)\cdots(p-k+1)$,且$(k!, p) = 1$,故有$(k!) \mid (p-1)\cdots(p-k+1)$.

因而$\frac{p(p-1)\cdots(p-k+1)}{k!} \equiv 0 (\mathrm{mod}\ p)$,所以$(a \pm b)^p = a^p \pm b^p$.

下设$e > 1$,且公式对$e - 1$成立,则

$(a \pm b)^{p^e} = \left[(a \pm b)^{p^{e-1}}\right]^p \overset{\text{由归纳假设}}{=} \left[a^{p^{e-1}} \pm b^{p^{e-1}}\right]^p = a^{p^e} \pm b^{p^e}$.

2. 设$Z[i]$为高斯整数环,求域$Z[i]/(2+i)$的特征.

解　令$F = Z[i]/(2+i)$,考虑元素$\bar{1}$在加群$(F, +)$中的阶:

由于　$5 = (2+i)(2-i) \in (2+i)$(注意后面的$(2+i)$是由$2+i$生成的理想),

故有　$\bar{5} = \bar{0}$.

所以　$o^+(\bar{1}) = 5$,　$chF = 5$.

3. 设p为素数,$(n, p) = 1$,则$n^{p-1} \equiv 1 (\mathrm{mod}\ p)$.

证　此题实际上在群论中可做.在域论中是要强调域$(F, +, \cdot)$中的加群$(F, +)$与乘群$(F^*, \cdot)$的性质.

考虑乘群$(Z_p^*, \cdot)$,由于$|Z_p^*| = p - 1$,因而

$\forall \bar{n} \in Z_p^*$有$(\bar{n})^{p-1} = \bar{1}$,写成整数形式为

对$(n, p) = 1$有$n^{p-1} \equiv 1 (\mathrm{mod}\ p)$.

4. 求$f(x) = x^2 + 1 \in Z_3[x]$在$Z_3$上的分裂域。

解　熟悉分裂域的概念和利用本节定理1的结果。

由于$f(x)$在$Z_3[x]$中不可约，由本节定理1,$Z_3[x]/(x^2+1)$是域，且$\alpha = x + (x^2+1)$是$f(x)$在此域上的根，且有$Z_3(\alpha) \cong Z_3[x]/(x^2+1)$,　$(Z_3(\alpha) : Z_3) = 2$。

另一方面，易见$(E_f : Z_3) = 2$,

5. 设K是F上的扩域,$a, b \in K$分别是F上的m次和n次代数元,证明

$(F(a,b) : F) \leq mn$,且当$(m, n) = 1$时等式成立.

证　本题的目的是熟悉代数元的概念.

由于a是F上的m次代数元,可设a的最小多项式为

$f(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_1x + a_0 \in F[x]$.

由于b是F上的n次代数元,可设b的最小多项式为

$g(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_1x + b_0 \in F[x]$.

令$E = F(a)$,则$g(x) \in E[x]$, $F(a,b) = E(b)$.并得$(E(b) : E) \leq n$.于是由域的望远镜公式得

$(F(a,b) : F) = (F(a,b) : F(a))(F(a) : F) = (E(b) : E)(F(a) : F) \leq mn$.　　(*)

再证第二个结论.

由式(*)可得 $m \mid (F(a,b) : F)$,类似可得$n \mid (F(a,b) : F)$,又由$(m, n) = 1$得$mn \mid (F(a,b) : F)$

综上得$(F(a,b) : F) = mn$.

6. 设Q为有理数域,

(1)求$u\in Q(\sqrt{2},\sqrt[3]{5})$使$Q(u)=Q(\sqrt{2},\sqrt[3]{5})$.

(2)求$w\in Q(\sqrt{2},\sqrt[3]{5})$使$Q(w)\neq Q(\sqrt{2},\sqrt[3]{5})$的条件是什么?

解　这个问题涉及到如何把一个添加有限个元素的扩张表为单扩张通常的方法是用线性组合的方法对于简单的情况可直接观察,但必须严格证明.

(1)观察可取$u=\sqrt{2}\sqrt[3]{5}$.

因为$u\in Q(\sqrt{2},\sqrt[3]{5})$,故$Q(u)\subseteq Q(\sqrt{2},\sqrt[3]{5})$.

反之,由于　$u^3=10\sqrt{2}$, 得$\sqrt{2}\in Q(u)$,

$u^4=20\sqrt[3]{5}$, 得$\sqrt[3]{5}\in Q(u)$.

故有　$Q(\sqrt{2},\sqrt[3]{5})\subseteq Q(u)$.

综上得　$Q(u)=Q(\sqrt{2},\sqrt[3]{5})$.

(2)我们从扩张次数入手.

由于$Q(w)\subseteq Q(\sqrt{2},\sqrt[3]{5})$,$(Q(\sqrt{2},\sqrt[3]{5}):Q)=6$,要使$Q(w)\neq Q(\sqrt{2},\sqrt[3]{5})$,必须使$Q(w)$的真子域,因而$(Q(w):Q)=1$,或2,或3.于是$w$必为

$w=a+b\sqrt{2},\quad a,b\in Q$

或

$w=a+b\sqrt[3]{5}+c\sqrt[3]{25},\quad a,b,c\in Q$.

7. 设正整数$m_1,m_2,(m_1,m_2)=1$,若正m_1边形与m_2边形可作出,则m_1m_2边形可作出.

证　方法一、考虑复平面上的点是否可作出。

由于正m_1边形与m_2边形可作出,复平面上点$e^{\frac{2\pi i}{m_1}}$和点$e^{\frac{2\pi i}{m_2}}$可作出。又由于$(m_1,m_2)=1$, 存在$p,q\in Z$使$pm_1+qm_2=1$。又因$\left(e^{\frac{2\pi i}{m_1}}\right)^q=e^{\frac{2q\pi i}{m_1}}$和$\left(e^{\frac{2\pi i}{m_2}}\right)^p=e^{\frac{2p\pi i}{m_2}}$可作出,

所以　$\left(e^{\frac{2\pi i}{m_1}}\right)^q+\left(e^{\frac{2\pi i}{m_2}}\right)^p=e^{\frac{2(pm_1+qm_2)\pi i}{m_1m_2}}=e^{\frac{2\pi i}{m_1m_2}}$可作出，即$m_1m_2$边形可作出.

方法二、本节最后提到，在4.4节中有分圆问题的完全解答，我们不妨翻到4.4节，提前用一下该定理：n边形可作出$\Leftrightarrow n=2^r p_1p_2\cdots p_s, p_i$为不同的费尔马素数。

由于正m_1边形可作出,得$m_1=2^r p_1p_2\cdots p_s,p_i$为不同的费尔马素数。

由于正m_2边形可作出,得$m_2=2^t q_1q_2\cdots q_u,q_j$为不同的费尔马素数。因为$(m_1,m_2)=1$.

故$p_i,1\le i\le s,q_j,1\le j\le u$互不相同,得$m_1m_2=2^{r+t}p_1p_2\cdots p_s q_1q_2\cdots q_u,p_i,q_j$为不同的费尔马素数,所以$m_1m_2$边形可作出.

8. 证明72°角可三等分.

证　应用角可三等分定理.

首先利用初等数学的方法可求出$\cos 72^\circ=\frac{\sqrt{5}-1}{4}$(利用底角为$72^\circ$的等腰三角形).

令$x=\cos 24^\circ$,则x可作出的充分必要条件是下列方程

$4x^3-3x-\frac{\sqrt{5}-1}{4}=0$

在$Q(\cos 72^\circ)=Q(\sqrt{5})$上可约.

用试根法或用代定系数法可求出此方程$Q(\sqrt{5})$上有根$-\frac{\sqrt{5}+1}{2}$。

所以72°角可三等分。

9. 设$a,b\in Z,|a|<|b|,\cos\theta=\frac{4a^3-3ab^2}{b^3}$,证明$\theta$角可三等分.

证　应用角可三等分定理.

令$x=\cos\theta/3$,则x可作出的充分必要条件是下列方程

$4x^3-3x-\frac{4a^3-3ab^2}{b^3}=0$

在$Q(\cos\theta)=Q(\frac{a}{b})$上可约.

用试根法或用代定系数法可求出此方程在$Q(\frac{a}{b})$上有根$\frac{a}{b}$。

所以θ角可三等分。

第4章 习题4.2 第1题解答

1. $f(x)\in F[x],\deg f(x)=n\Rightarrow(E_f:F)\le n!$。

证　掌握分裂域的概念。

对n作归纳法。

$n=1$,显然成立。

下设$n>1$,并设结论$n-1$成立。

由于$f(x)$在其分裂域E_f上必有根，设有根α，令

$f(x)=(x-\alpha)f_1(x)$,则$\deg f_1(x)=n-1$,且$f_1(x)\in F(\alpha)[x]$，由归纳假设，得$(E_{f_1}:F(\alpha))\le(n-1)!$。注意到$(F(\alpha):F)\le n$和$E_{f_1}=E_f$,由望远镜公式得$(E_f:F)=(E_f:F(\alpha))(F(\alpha):F)\le n!$。

2. $p(x)\in F[x]$不可约, $E=F[x]/(p(x))$, $u=x+(p(x))\in E$,证明$p(u)=0$。

证　熟悉商环的概念及其元素的表示方法，同余类的运算等。

首先E是域，对于任何一个多项式$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\in F[x]$有

$f(x+(p(x)))=a_n(x+(p(x)))^n+a_{n-1}(x+(p(x)))^{n-1}+\cdots+a_1(x+(p(x)))+a_0=f(x)+(p(x))$,

所以$p(x+(p(x)))=p(x)+(p(x))=0+(p(x))=\bar{0}$。

3. 确定下列多项式在Q上的分裂域及其次数。

(1)　x^6+1.

(2)　$x^5-2x^3-2x^2+4$.

(3)　x^p-1, p为素数。

解　掌握分裂域的概念和表示方法。

(1)　$x^6+1=(x^2+1)(x^4-x^2+1)$,可求出此多项式的根为

$x_{1,2}=\pm i,\quad x_{3,4}=\pm\frac{1-\sqrt{3}i}{2i},\quad x_{5,6}=\pm\frac{1+\sqrt{3}i}{2i}$.

所以得　$E_f=Q(\sqrt{3},i)$,　$(E_f:Q)=4$.

(2)　$x^5-2x^3-2x^2+4=(x^2-2)(x^3-2)$,可求出此多项式的根为

$x_{1,2}=\pm\sqrt{2},\quad x_3=\sqrt[3]{2},\quad x_{4,5}=\frac{\sqrt[3]{2}(-1\pm\sqrt{3}i)}{2}$.

不难证明　$E_f=Q(\sqrt{2},\sqrt[3]{2},\sqrt{3}i)$,

所以　$(E_f:Q)=12$.

(3)　$x^p-1=(x-1)\Phi_p(x)$,其中$\Phi_p(x)$为p次分圆多项式。设ω是$\Phi_p(x)$的一个根，则$\Phi_p(x)$的所有根都在$Q(\omega)$中，所以　$E_f=Q(\omega)$,　$(E_f:Q)=(Q(\omega):Q)=p-1$。

4. 求$f(x)=x^2+1\in Z_3[x]$在Z_3上的分裂域。

解 熟悉分裂域的概念和利用本节定理的结果。

由于$f(x)$在$Z_3[x]$中不可约，由本节定理1, $Z_3[x]/(x^2+1)$是域，且$\alpha=x+(x^2+1)$是$f(x)$在此域上的根，且有$Z_3(\alpha)\cong Z_3[x]/(x^2+1)$, $(Z_3(\alpha):Z_3)=2$。

另一方面，易见$(E_f:Z_3)=2$,

5. $f(x)\in F[x]$不可约，$chF=0$, 证明$f(x)$在其分裂域上无重根。

证 利用多项式有重根的条件。

因$f(x)$在F上不可约，又由于$chF=0$，得$\deg f'(x)=n-1$,故在F上$(f(x),f'(x))=1$，此式在$f(x)$的分裂域E_f上也成立（从最大公因子定理可见）。所以$f(x)$在其分裂域上无重根。

（如果$chF\neq 0$，则$\deg f'(x)=n-1$不一定成立。）

6. $chF=p$，多项式$f(x)\in F(x)$不可约，证明$f(x)$在E_f上有重根$\Leftrightarrow f(x)$可表为x^p的多项式。

证 利用多项式有重根的条件。

$\Rightarrow$：$f(x)$在E_f上有重根，则$(f(x),f'(x))\neq 1$。但因 $\deg f'(x)<\deg f(x)$和$f(x)$不可约，必有 $f'(x)=0$，设

$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$,

则

$f'(x)=na_nx^{n-1}+(n-1)a_{n-1}x^{n-2}+\cdots+a_1$,

由$f'(x)=0$得 $ka_k=0, k=1,\cdots,n$.

因而当$k\neq 0$时有$a_k=0$。由于$chF=p$，得$k\neq 0(\mathrm{mod}\ p)$时有$a_k=0$,

所以 $f(x)=g(x^p)$。

$\Leftarrow$：$f(x)$可表为x^p的多项式。

则 $f'(x)=0$, $(f(x),f'(x))=f(x)\neq 1$，所以$f(x)$有重根。

第 4 章 习题 4.3 第 1 题解答

1. 证明

(1) $(F_{p^n}:F)=n$.

(2) $\forall u\in F_{p^n}$有$(Z_p(u):Z_p)|n$.

证 熟悉有限域的不同的表示方法和基本性质。

(1) 考虑有限域的商环表示。任取一个Z_p上的n次不可约多项式$p(x)$,

则 $F_{p^n}\cong Z_p[x]/(p(x))$, 所以 $(F_{p^n}:F)=n$。

(2) 利用有限域的子域的性质（定理4）。

由于$Z_p(u)$是F_{p^n}的子域，由定理4，得必有某个m：$m|n$ 使 $Z_p(u)=F_{p^m}$。

又有上面已证明的 (1) ，得 $(Z_p(u):Z_p)=(F_{p^m}:F)=m$,

所以 $(Z_p(u):Z_p)|n$。

2. 构造125和64个元素的有限域，并用图形表示它的子域。

解 掌握有限域的构造方法。

(1)$125=5^3$,在$Z_5[x]$中取一3次不可约多项式，例如

$f(x)=x^3+x+1$,

对3次多项式要判断是否可约最容易了，只要检验它在Z_5上是否有根。

得域 $GF(5^3)=Z_5[x]/(x^3+x+1)$,就是125阶域。

$GF(5^3)$的非平凡子域只有$GF(5)$。

(2)$64=2^6$，在$Z_2[x]$中取一6次不可约多项式，例如

$f(x)=x^6+x+1$,

要证明它不可约，需费一些工夫。

得域 $GF(2^6)=Z_2[x]/(x^6+x+1)$,就是64阶域。

$GF(2^6)$的非平凡子域有$GF(2)$, $GF(2^2)$, $GF(2^3)$。

3. p为素数$\Rightarrow (p-1)!\equiv -1(\mathrm{mod}\ p)$。

证 涉及$\mathrm{mod}\ p$的同余式的问题，可考虑在$chF=p$的有限域中求解。

考虑有限域Z_p上的多项式, $f(x)=x^{p-1}-1\in Z_p[x]$, 由于$1,2,\cdots,p-1$恰是$f(x)$的$p-1$个根，故有

$f(x)=x^{p-1}-1=(x-1)(x-2)\cdots(x-(p-1))$,

比较两边的常数项得 $(p-1)!=-1$, 这是域中的等式，写成整数形式即为

$(p-1)!\equiv -1(\mathrm{mod}\ p)$。

4. 求多项式$f(x)=x^3+2x+1\in Z_3[x]$在它的分裂域中的全部根。

解 根据本节定理3，首先将$f(x)$分解为不可约因式，然后求出每一个不可约因式的所有根。

很易证明$f(x)=x^3+2x+1$在$Z_3[x]$上不可约。又由已知的定理, $\bar{x}=x+(f(x))$是$f(x)$在其分裂域上的一个根，根据本节定理3，$f(x)$的全部根为

$\bar{x}=x+(f(x))$, $\bar{x}^3=x^3+(f(x))$, $\bar{x}^9=x^9+(f(x))$

可以化简为

$\alpha_1=\bar{x}$, $\alpha_2=\overline{x+2}$, $\alpha_3=\overline{2x^2-x}$。

5. 求$E=Z_3[x]/(x^2+1)$的所有本原元.

解 复习本原元的概念

$E=Z_3[x]/(x^2+1)=GF(3^2)=\{0,1,2,x,2x,x+1,x+2,2x+1,2x+2\}$,

其中元素均为模(x^2+1)的同余类,为简单起见,不用同余类的记号.它们的运算也是模(x^2+1)的运算.

本原元即为乘法阶为$3^2-1=8$的元素.先算一下本原元的个数,由本节结果,知$GF(3^2)$中本原元的个数为$\varphi(3^2-1)=\varphi(8)=4$.对$GF(3^2)$的元素逐个进行计算,可得$GF(3^2)$中全部本原元为

$x+1$, $x+2$, $2x+1$, $2x+2$.

6. 设$q(x)$是Z_p上的n次首1不可约多项式，则

$q(x)$是Z_p上的n次本原多项式$\Leftrightarrow q(x)|x^{p^n-1}-1$,但$q(x)$不能整除$x^m-1,\forall m<p^n-1$.

证 熟悉本原多项式的概念：n次本原元的最小多项式。

$\Rightarrow$：设$q(x)$是Z_p上的n次本原多项式，它的根都是n次本原元，都在$GF(p^n)$中，因而$q(x)|x^{p^n-1}-1$。

若有$m<p^n-1$使$q(x)|(x^m-1)$,任取$q(x)$的一个根α，则$\alpha^m=1$，则与$o^*(\alpha)=p^n-1$矛盾。所以，$\forall m<p^n-1$有$q(x)$不能整除x^m-1。

$\Leftarrow$：设$q(x)|x^{p^n-1}-1$,但$q(x)$不能整除$x^m-1,\forall m<p^n-1$，可令$x^{p^n-1}-1=p(x)q(x)$，任取$q(x)$的一个根α，则$\alpha^{p^n-1}=1$，但$\forall m<p^n-1$有$\alpha^m\neq 1$，故α是n次本原元，所以$q(x)$是Z_p上的n次本原多项式

7. 设$I_p(n)Z_p$上n次不可约首1多项式的个数，证明

(1) $p^n=\sum_{m|n} mI_p(m)$.

(2) 由$Mobius$反演公式：$f(n)=\sum_{d|n} g(d) \Rightarrow g(n)=\sum_{d|n}\mu(d)f\left(\frac{n}{d}\right)$ 求$I_p(n)$的公式。

证　通过该题进一步了解有限域的每一个元素的性质和$Mobius$反演公式的应用。

(1) 由于$\left|GF(p^n)\right|=p^n$,所以要证明该题，就是找到$GF(p^n)$中的元素的最小多项式的性质。

设α是$GF(p^n)$中的任一元素，则$Z_p(\alpha)$是$GF(p^n)$的一个子域，由有限域的子域的性质，得　$Z_p(\alpha)=GF(p^m)$且$m|n$，故α是某个$m(m|n)$次多项式的根。反之，任何一个$m(m|n)$次不可约多项式的根均在$GF(p^n)$中，且任何两个不可约多项式没有相同的根。综上得

$p^n=\sum_{m|n} mI_p(m)$。

(2) 由$Mobius$反演公式得

$nI_p(n)=\sum_{d|n}\mu(d)p^{\frac{n}{d}}$,

所以有

$I_p(n)=\frac{1}{n}\sum_{d|n}\mu(d)p^{\frac{n}{d}}$。

8. 求Z_2上所有4次不可约多项式和本原多项式。并说明判断一个不可约多项式是否是本原多项式不的方法。

解　首先计算4次不可约多项式和本原多项式的个数，然后对$x^{2^4-1}-1$分解因式，求出所有4次不可约多项式，从中排除非本原多项式。

由公式得4次不可约多项式的个数为

$$I_2(4)=\frac{1}{4}\sum_{d|4}\mu(d)2^{\frac{4}{d}}=\frac{1}{4}\left(\mu(1)2^4+\mu(2)2^2+\mu(4)2\right)$$

$$=\frac{1}{4}(16-4+0)=3,$$

4次本原多项式的个数为

$$J_2(4)=\varphi(2^4-1)/4=\varphi(15)/4=8/4=2.$$

对$x^{2^4-1}-1$分解因式：

$x^{2^4-1}-1=x^{15}-1=(x^5-1)(x^{10}+x^5+1)=(x-1)(x^4+x^3+x^2+x+1)(x^{10}+x^5+1)$

$=(x-1)(x^4+x^3+x^2+x+1)(x^2+x+1)(x^8+x^7+x^5+x^4+x^3+x+1)$

$=(x-1)(x^4+x^3+x^2+x+1)(x^2+x+1)(x^4+x^3+1)(x^4+x+1)$,

得到3个不可约多项式为：

$q_1(x)=x^4+x^3+x^2+x+1$,

$q_2(x)=x^4+x^3+1$,

$q_3(x)=x^4+x+1$.

由于$q_1(x)\left|(x^5-1)\right.$，由本节习题第6题知$q_1(x)$不是本原多项式，所以4次本原多项式为

$q_2(x)=x^4+x^3+1$,

$q_3(x)=x^4+x+1$.

9. 证明$GF(p^n)$中每个元素都是p次幂也是p次方根。

证　利用$GF(p^n)$上的自同构。

考虑$GF(p^n)$上的变换 $f:\alpha\mapsto\alpha^p$,

由本节性质（1），知f是$GF(p^n)$上的自同构。因而

$\forall u\in GF(p^n),\exists\alpha\in GF(p^n)$使$u=\alpha^p$,所以$GF(p^n)$中每个元素都是$p$次幂。

另一方面，$\forall u\in GF(p^n)$，$f(u)=u^p\in GF(p^n)$,令$u^p=\beta$，则u是β的p次方根。所以$GF(p^n)$中每个元素都是p次根。

10. 证明$Z_p[x]$中全部n次不可约多项式和n次本原多项式可通过分解$f(x)=x^{p^n}-x$成不可约因式得到。

证　我们在前面已用到这个结论。

设$p(x)$是$Z_p[x]$中任一个n次不可约多项式，它的全部根都在$GF(p^n)$中，故得　$p(x)|f(x)$。由于不同的n次不可约多项式无相同的根，设有s个n次不可约多项式：$p_1(x),p_2(x),\cdots,p_s(x)$,则它们互素，故

$p_1(x)p_2(x)\cdots p_s(x)|f(x)$,

又由于$Z_p[x]$是唯一分解环，所以$p_1(x),p_2(x),\cdots,p_s(x)$可通过分解$f(x)=x^{p^n}-x$成不可约因式得到。

全部n次本原多项式可从全部n次不可约多项式中选取。

第4章 习题4.4 第1题解答

1. 写出$\Phi_5(x)$和$\Phi_6(x)$.

解　复习分圆多项式的概念和求的方法。

n次分圆多项式$\Phi_n(x)$是以n次原根为根的多项式，它的次数为$\varphi(n)$。可通过分解x^n-1得到。

(1) 由于5是素数，故$\Phi_5(x).=x^4+x^3+x^2+x+1$.

(2) $\varphi(6)=2$，故$\deg\Phi_6(x)=2$.

$x^6-1=(x^3-1)(x^3+1)=(x-1)(x^2-x+1)(x+1)(x^2+x+1)$,

所以得

$\Phi_6(x)=x^2+x+1$。

2. 证明　$x^n-1=\prod_{d|n}\Phi_d(x)$.

证　利用两边可互相整除来证明相等。

x^n-1在C上的全部根的集合为　$G=\left\{e^{\frac{2\pi}{n}i}\middle| i=0,1,\cdots,n-1\right\}$　,

$\forall\alpha\in G$,设$o^*(\alpha)$是α的乘法阶，则$o^*(\alpha)|n$，令$d=o^*(\alpha)$,则α是$\Phi_d(x)$的根。故有$(x^n-1)\left|\prod_{d|n}\Phi_d(x)\right.$。

反之，对任何$\Phi_d(x),d|n$的根都是x^n-的根，故有$\Phi_d(x)\left|(x^n-1)\right.$。又，不同的分圆多项式无相同的根，因此$\prod_{d|n}\Phi_d(x)\left|(x^n-1)\right.$。

综上，等式成立。

3. 证明85边形可作出。

证　简单运用n边形可作出定理。

由于　$85=5\times7$,

其中　$5=2^2+1$，　$17=2^{2^2}+1$　均为$Fermat$素数，所以85边形可作出。

4. 利用分圆多项式的根作出正五边形。

解　我们在习题1.1中已经用初等数学的方法做过此题，现我们用分圆多项式再来做。

$n=5$的分圆多项式为

$$\Phi_5(x)=x^4+x^3+x^2+x+1,$$

设α是一个根，则

$$\alpha^4+\alpha^3+\alpha^2+\alpha+1=0,$$

$$\left(\alpha^2+\frac{1}{\alpha^2}\right)+\left(\alpha+\frac{1}{\alpha}\right)+1=0,$$

令　$y=\alpha+\frac{1}{\alpha}=e^{\frac{2\pi}{5}i}+e^{-\frac{2\pi}{5}i}=2\cos\frac{2\pi}{5}$，则$y$满足方程

$$y^2+y-1=0,$$

得正解　$y=\frac{\sqrt{5}-1}{2}$，进一步得

$$\cos\frac{2\pi}{5}=\frac{\sqrt{5}-1}{4},$$

从而可作出正五边形。

补充题第一部分

补充题第一部分(预备知识)　习题解答

补充题：n维欧氏向量空间中有且最多有$n+1$个互夹钝角的向量.

证：

(1)先证存在性。对n作归纳。$n=1$显然成立。

下设$n>1$,由归纳假设，R^{n-1}中有n个互夹钝角的向量：

$\alpha_i=(a_{i1},a_{i2},\ldots\ldots,a_{in-1},b)$,　　$i=1,2,\ldots\ldots n$　　且$(\alpha_i,\alpha_j)<0$　$(i\neq j)$

在R^n中取$\beta_i=(a_{i1},a_{i2},\ldots\ldots,a_{in-1},b)$　$,i=1,2,\ldots\ldots,n$

$\beta_{n+1}=(0,0,\ldots\ldots,0,-1)$

其中$0<b<\sqrt{\max\limits_{1\le i<j\le n}|(\alpha_i,\alpha_j)|}$

则有　$(\beta_i,\ \beta_j)<0$,　$1\le i<j\le n+1$

(2)再证最多存在$n+1$个互夹钝角的向量。

对n作归纳法。$n=1$显然成立。　下设$n>1$

反证法。假设R^n中有$\alpha_1,\alpha_2,\ldots\ldots,\alpha_{n+2}$互夹钝角，取一组标准正交基$\varepsilon_1.\varepsilon_2,\ldots\ldots\varepsilon_{n-1}.\varepsilon_n=\alpha_{n+2}$

则可设　　$\alpha_i=(a_{i1},\ldots\ldots,a_{i,n-1},b_i)$,　$i=1,2,\ldots\ldots,n+1.$

$\alpha_{n+2}=(0,\ldots\ldots,0,1)$,

由$(\alpha_i,\alpha_j)<0,(i\neq j)$,得$b_i<0$,　$\sum\limits_{k=1}^{n-1}a_{ik}a_{jk}<-b_ib_j$　　$(1\le i<j\le n+1)$

取$\beta_i=(a_{i1},a_{i2},\ldots\ldots,a_{i,n-1})$,$i=1,2,\ldots\ldots,n+1$

则$(\beta_i,\beta_j)=\sum\limits_{i=1}^{n-1}a_{ik}a_{jk}<0$　$(1\le i<j\le n+1)$,

即$\beta_1,\beta_2,\ldots\ldots,\beta_{n+1}$在$R^{n-1}$中互夹钝角，与归纳假设矛盾。

存在性证明的直接方法

$$\alpha_1=\left(-1,\frac{1}{n},\ldots\ldots,\frac{1}{n}\right)^T$$

$$\alpha_2=\left(\frac{1}{n},-1,\ldots\ldots,\frac{1}{n}\right)^T$$

$\vdots$

$$\alpha_n=\left(\frac{1}{n},\frac{1}{n},\ldots\ldots,\frac{1}{n},-1\right)^T$$

$$\alpha_{n+1}=\left(\frac{1}{\sqrt{n}},\frac{1}{\sqrt{n}},\ldots\ldots,\frac{1}{\sqrt{n}}\right)^T$$

则$(\alpha_i,\alpha_j)=-\frac{2}{n}+\frac{n-2}{n^2}=\frac{-n-2}{n^2}<0,(1\le i<j\le n)$

$(\alpha_i,\alpha_j)=\frac{n-1}{n\sqrt{n}}-\frac{1}{\sqrt{n}}=-\frac{1}{n\sqrt{n}}<0$

补充题：证明3维几何空间中正n面体只有5种.

证：

(1)设面数为n,每面为正m边形,每个顶点与k条边相连.

则顶点数为$\frac{mn}{k}$,边数为$\frac{mn}{2}$，代入欧拉公式：

$$\frac{mn}{k}-\frac{mn}{2}+n=2$$

$$得n=\frac{4k}{2m+2k-mk}$$

(2)求整数解

$m=3$,　$n=\frac{4k}{6-k}$,得

$k=3,n=4$;　$k=4,n=8$;　$k=5,n=20$

$m=4$,　$n=\frac{2k}{4-k}$,得

$k=3,n=6$;

$m=5$,　$n=\frac{4k}{10-3k}$,得$k=3,n=12$;

$m=6$,　$n=\frac{4k}{12-4k}$,无解.

$\therefore n=4,6,8,12,20$　　共五种.

补充题：由两个2阶元生成的有限群同构于K_4或$D_n(n\ge 3)$.

证：　设$G=\langle a,b\rangle$　　$o(a)=o(b)=2$,　$|G|<\infty$

令$r=ab$,由$|G|<\infty$,　　可设$o(r)=n$

(1)当$n=2$,　　则$G=\{e,a,b,ab\}\cong K_4$

(2)当$n\ge 3$,　　由于$br=bab=(ab)^{-1}b=r^{-1}b$,因而$G$可表为

$G\ =\{r^k,r^kb\,|\,k=0,1,\ldots\ldots,n\}$

$=\langle r,b\,|\,o(r)=n,o(b)=2,且br=r^{-1}b\rangle\cong D_n$

题：

(1)设$G_1=\left\{\begin{pmatrix}1&n\\0&\pm1\end{pmatrix}\Big|\,n\in Z\right\}$是关于矩阵乘法的群,证明$G_1$可以由两个2阶元生成.

(2)由两个2阶元生成的无限群 同构于G_1.

证：

(1)令$A=\begin{pmatrix}1&0\\0&-1\end{pmatrix}$,$B=\begin{pmatrix}1&1\\0&-1\end{pmatrix}$　　则$o(A)=o(B)=2$

显然$\langle A,B\rangle\subseteq G_1$

反之，　由于$AB=\begin{pmatrix}1&1\\0&1\end{pmatrix}=R$,　$R^n=\begin{pmatrix}1&n\\0&1\end{pmatrix}$,$AR^n=\begin{pmatrix}1&n\\0&-1\end{pmatrix}$

$\therefore G_1\subseteq<A,B>$

(2)设$G=\langle a,b\rangle,o(a)=o(b)=2,|G|=\infty$

令$r=ab$,　　则$ra=aba=ar^{-1}$,G可表为$G=\{r^n,ar^n\mid n\in Z\}$

而$G_1=\{R^n,AR^n\mid n\in Z\}$

$\therefore G\cong G_1$

补充题：$a\ ,b\in G,ab=ba,o(a)=m,o(b)=n$,且$\langle a\rangle\cap\langle b\rangle=\{e\}$,则$o(ab)=mn/(m,n)$

证法1：　　令$o(ab)=k$,　$[m,n]=mn/(m,n)$
由于$(ab)^{[m,n]}=a^{[m,n]}b^{[m,n]}=e$
得$k\mid[m,n]$
另由 $(ab)^k=a^kb^k=e$,
得$a^k=b^{-k}$
由$<a>\cap<b>=\{e\}$,得
$a^k=b^{-k}=e$
$\therefore m\mid k, n\mid k$,
综上得$o(ab)=k=[m,n]$.
证法2：令$o(ab)=k, d=(m,n), m=m_1d, n=n_1d, (m_1,n_1)=1$
由$(ab)^{\frac{mn}{d}}=a^{m\frac{n}{d}}b^{n\frac{m}{d}}=e$,得$k\left|\frac{mn}{d}\right., k\mid m_1n_1d$
反之，由$(ab)^{km}=b^{km}=e\Rightarrow n_1\mid k$,同理$m_1\mid k$
可令：$k=m_1n_1d_1, (ab)^k=a^kb^k=e$
综上得：$k=dm_1n_1=\frac{mn}{(m,n)}$

补充题：证明$AutD_n\cong\left\{\begin{pmatrix}1&0\\b&a\end{pmatrix}\mid a\in Z_n^*, b\in Z_n\right\}$　　$n\geq 3$

证：
(1)首先确定$AutD_n$　　$D_n=\{\rho_i,\pi_i\mid i=0,1,\ldots\ldots,n-1\}=\langle\rho_1,\pi_0\rangle$
设φ为D_n上任意一个同构，则有
$\varphi(\rho_1)=\rho_k,(k,n)=1$　　$\varphi(\pi_0)=\pi_l, l=0\ldots n-1$
则$AntD_n=\{\varphi_{k,l}\mid(k,n)=1,k,l=0\ldots n-1\}$
(2)令$G=\left\{\begin{pmatrix}1&0\\b&a\end{pmatrix}\mid a\in Z_n^*, b\in Z_n\right\}$
$f:\varphi_{k,l}\mapsto\begin{bmatrix}1&0\\l&k\end{bmatrix}$　$(AutD_n\to G)$
显然f是双射。　易证
$\varphi_{k_1l_1}\varphi_{k_2l_2}=\varphi_{k_1k_2,k_1l_2+l_1}$　$\begin{pmatrix}1&0\\l_1&k_1\end{pmatrix}\begin{pmatrix}1&0\\l_2&k_2\end{pmatrix}=\begin{pmatrix}1&0\\k_1l_2+l_1&k_1k_2\end{pmatrix}$
$\therefore f(\varphi_{k_1,l_1}\cdot\varphi_{k_2,l_2})=f(\varphi_{k_1,l_1})f(\varphi_{k_2,l_2})$
$\therefore AutD_n\cong G$

补充题：证明$AutZ[X]\cong\left\{\begin{pmatrix}1&b\\0&\varepsilon\end{pmatrix}\mid\varepsilon=\pm1, b\in Z\right\}$

证：
(1) $\forall\sigma\in AutZ[X]$,确定σ的性质：
$\because Z[X]=(1,X)$,　$\because\sigma(1)=1$,　所以$\sigma(a)=a$,　$a\in Z$
可证$\sigma(X)=aX+b$,否则与σ满射矛盾
$\exists cX+d$,使$\sigma(cX+d)=X, c(aX+b)+d=x$;得$ac=1,\therefore a=1$或$-1$
故$\sigma(X)=\varepsilon X+b,\varepsilon=\pm1,b\in Z$
因而σ可表为$\sigma_{\varepsilon,b}(f(X))=f(\varepsilon X+b)$
(2)写出$AutZ[X]$
由(1),$AutZ[X]=\{\sigma_{\varepsilon,b}\mid\varepsilon=\pm1,b\in Z,\sigma_{\varepsilon,b}(f(X))=f(\varepsilon X+b)\}$
(3)证明$AutZ[X]\cong\left\{\begin{pmatrix}1&b\\0&\varepsilon\end{pmatrix}\mid\varepsilon=\pm1,b\in Z\right\}$
(主要证保运算）　　$\varphi:\sigma_{\varepsilon,b}\mapsto\begin{pmatrix}1&b\\0&\varepsilon\end{pmatrix}$易证是双射
$\sigma_{\varepsilon1,b1}\sigma_{\varepsilon2,b2}(f(X))=\sigma_{\varepsilon1,b1}(f(\varepsilon_2X+b_2)=f(\varepsilon_2(\varepsilon_1X+b_1)+b_2)$
$\varphi(\sigma_{\varepsilon1,b1})\varphi(\sigma_{\varepsilon2,b2})=\begin{pmatrix}1&b_1\\0&\varepsilon_1\end{pmatrix}\begin{pmatrix}1&b_2\\0&\varepsilon_2\end{pmatrix}=\begin{pmatrix}1&b_2+\varepsilon_2b_1\\0&\varepsilon_1\varepsilon_2\end{pmatrix}$
$\therefore\varphi(\sigma_{\varepsilon1,b1}\sigma_{\varepsilon2,b2})=\varphi(\sigma_{\varepsilon1,b1})\varphi(\sigma_{\varepsilon2,b2})$
$\therefore AutZ[X]=\{\sigma_{\varepsilon,b}\mid\varepsilon=\pm1,b\in Z\}$.

补充题：$SL(2,Z)$可由一个3阶元与一个5阶元生成

证：取$Q=\begin{pmatrix}0&1\\-1&0\end{pmatrix}$　　$P=\begin{pmatrix}-1&-1\\1&0\end{pmatrix}$, $o(Q)=4, o(P)=3$
$\because SL(2,Z)=<A,B>$　　$A=\begin{pmatrix}1&1\\0&1\end{pmatrix}$　$B=\begin{pmatrix}1&0\\1&1\end{pmatrix}$
$\because B^{-1}AB^{-1}=Q, A^{-1}BA^{-1}=Q^T, Q^TB=P$
$\therefore<Q,P>\subseteq<A,B>$
另一方面$QP=\begin{pmatrix}1&0\\1&1\end{pmatrix}=B, PQ=\begin{pmatrix}1&-1\\0&1\end{pmatrix}=A^{-1}\Rightarrow Q^{-1}P^{-1}=A$
$\therefore<Q,P>\supseteq<A,B>$
$\therefore SL(2,Z)=<P,Q>$

补充题：O_3中任一旋转变换可表为两个2阶元之积（一个旋转可表为两个反射之积）

证：设A为旋转变换：$A=\sigma(n,\theta)$,令$c=\cos\theta, s=\sin\theta$
则存在正交矩阵P使$P^{-1}AP=\begin{bmatrix}c&-s&0\\s&c&0\\0&0&1\end{bmatrix}=\begin{bmatrix}-1&0&0\\0&1&0\\0&0&1\end{bmatrix}\begin{bmatrix}-c&s&0\\s&c&0\\0&0&1\end{bmatrix}$
则$A=BC$,　　$B=P\begin{bmatrix}-1&0&0\\0&1&0\\0&0&1\end{bmatrix}P^{-1}$,　　, $C=P\begin{bmatrix}-c&s&0\\s&c&0\\0&0&1\end{bmatrix}P^{-1}$
$B^2=C^2=E$,　　$B,C\in O_3$

补充题第二部分(环论) 习题解答

引理1：设α为$Z[i]$中的既约元，则α能且只能整除一个素数。

证：设$\alpha=a+bi$, $\nu(\alpha)=\alpha\bar{\alpha}=a^2+b^2=p_1p_2\ldots p_s$, p_i为素数，
由$Z[i]$的唯一分解性，α为素元，故必有某个p_i使$\alpha\mid p_i$.
在证唯一性：设$\alpha\mid p$,(p为素数),则$\bar{\alpha}\mid p$，因而得$p=\alpha\bar{\alpha}$,
故p由α唯一决定。

引理2：设$\alpha\in Z[i]$且$\nu(\alpha)=a^2+b^2$素数，则α是既约元。

证：由于$U(Z[i])=\{1,-1,i,-i\}$
$\forall\beta\in Z[i]^*\setminus U(Z[i])$　有$\nu(\beta)>1$
设$\alpha=\alpha_1\alpha_2$
$\nu(\alpha)=\nu(\alpha_1)\nu(\alpha_2)=$素数,
故必有$\nu(\alpha_1)=1$或$\nu(\alpha_2)=1$
即$\alpha_1\in U(Z[i])$或$\alpha_2\in U(Z[i])$
$\therefore\alpha$为既约元

引理2'：设$\alpha=a+bi, ab\neq0$则α是既约元$\Leftrightarrow a^2+b^2=$素数。

证：$\Leftarrow$：由引理二
$\Rightarrow$：设$a+bi$为既约元，必有$(a,b)=1$，反证法，假设$a^2+b^2=pq, p>1, q>1$
可设p为素数　即$\alpha\bar{\alpha}=pq$,
$\because\alpha$为素元，由$\alpha\mid pq$得$\alpha\mid q$或$\alpha\mid q$
于是得$p=\alpha\bar{\alpha}$或$q=\alpha\bar{\alpha}$, $\therefore\alpha\bar{\alpha}=$素数

引理3：设p为大于2的素数，$a\neq0(\bmod p)$,
则$x^2\equiv a(\bmod p)$在Z中有解的充要条件是$a^{\frac{p-1}{2}}\equiv1(\bmod p)$

证：⇒：$x \equiv a(\mathrm{mod}\ p)$在$Z$中有解，设$b$是一个解：$b^2 \equiv a(\mathrm{mod}\ p)$,则

$a^{\frac{p-1}{2}} \equiv b^{p-1}(\mathrm{mod}\ p)$,由于$a \neq 0(\mathrm{mod}\ p) \Rightarrow b \neq 0(\mathrm{mod}\ p)$

$\therefore b^{p-1} \equiv 1(\mathrm{mod}\ p)$

⇐:$a^{\frac{p-1}{2}} \equiv 1(\mathrm{mod}\ p)$,

当$p = 4n+3$时，

$a^{\frac{p-1}{2}} = a^{2n+1} \equiv 1(\mathrm{mod}\ p)$故　　$a^{2n+2} = (a^{n+1})^2 \equiv a(\mathrm{mod}\ p)$

a^{n+1}是$x^2 \equiv a(\mathrm{mod}\ p)$的一个解.

当$p = 4n+1$时，由于$a \neq 0(\mathrm{mod}\ p), \bar{a} \notin Z_p^*$,

而$(Z_p^*, \bullet)$是循环群,可令$Z_p^* = \langle C \rangle, \bar{a} = \bar{C}^m$,

则$a^{\frac{p-1}{2}} = a^{2n} \equiv C^{2nm} \equiv 1(\mathrm{mod}\ p)$

由$o(C) = 4n$,得$4n \mid 2mn, 2 \mid m$.　　可令$m = 2l$

得$C^{2l} = (C^l)^2 \equiv a(\mathrm{mod}\ p)$

C^l就是$x^2 \equiv a(\mathrm{mod}\ p)$的解

引理4：若素数$p \equiv 1(\mathrm{mod}\ 4)$,则$p$不是$Z[i]$中的既约元。

证：设$p = 4n+1$,于是$(-1)^{\frac{p-1}{2}} = 1$,由习题3.5.6,

方程$x^2 = -1(\mathrm{mod}\ p)$有解，即有$a \in Z$使

$a^2 = -1(\mathrm{mod}\ p)$,即$a^2 + 1 = kp = (a+i)(a-i)$

于是得$p \mid (a+i)(a-i)$且p不整除$(a+i)$或$(a-i)$

$\therefore p$不是素元，也非即约元

引理5:　　若$a^2 + b^2 = p(素数) > 2$,则$p \equiv 1(\mathrm{mod}\ 4)$

证：首先可见a与b的奇偶性相反，否则$a^2 + b^2 \neq$素数

因而可令$a = 2n, b = 2n+1$

$\therefore a^2 + b^2 = 4n^2 + 4n^2 + 4n + 1 \equiv 1(\mathrm{mod}\ 4)$

习题 3.7 解答

写出由 p(x)=1+x2+x3 生成的所有（6，3）码。

解　作下表：

信息	信息多项式 m(x)	x3m(x)	r(x): x3m(x)=q(x)p(x)+r(x)	v(x)= r(x)+ x3m(x)	码词
000	0	0	0	0	000000
100	1	x3	1+x2	1+ x2+ x3	101100
010	x	x4	1+x+x2	1+ x+ x2+x4	111010
001	x2	x5	1+x	1+x+ x5	110001
110	1+x	x3+ x4	x	x+ x3+ x4	010110
101	1+ x2	x3+ x5	x+ x2	x+ x2+ x3+ x5	011101
011	x+ x2	x4+ x5	x2	x2+ x4+ x5	001011
111	1+x+ x2	x3+ x4+x5	1	1+ x3+ x4+x5	100111